



UNIVERSITY OF AMSTERDAM

MSc Computational Science

Master Thesis

Secure Identification in the Isolated Qubits Model

by

Filippos-Arthouros Vogiatzian-Ternaxizian
10661565

October 2015

Supervisor:
Dr. Christian Schaffner

Examiners:
Dr. Inge Bethke
Dr. Serge Fehr

Abstract

Oblivious transfer is a powerful cryptographic primitive that is complete for secure multi-party computation. In oblivious transfer protocols a user sends one or more messages to a receiver, while the sender remains oblivious as to which messages have been received. Protocols for oblivious transfer cannot exist in a classical or fully-quantum world, but can be implemented by restricting the users' power.

The isolated qubits model is a cryptographic model in which users are restricted to single-qubit operations and are not allowed to use entangling operations. Furthermore, all parties are allowed to store qubits for a long time before measuring them.

In this model, a secure single-bit one-out-of-two randomised oblivious transfer protocol was recently presented by Liu. Motivated by this result, we construct a protocol for secure string one-out-of-two randomised oblivious transfer by simplifying and generalising the existing proof.

We then study for the first time interactive protocols for more complex two-party functionalities in this model based on the security of our construction. In order to guarantee the composability of our construction, users are restricted to measurement at the end of each sub-protocol. It is then possible to construct secure one-out-of-two and one-out-of-k oblivious transfer protocols in the isolated qubits model.

Moreover, we study secure password-based identification, where a user identifies himself to another user by evaluating the equality function on their inputs, or passwords. We use the oblivious transfer constructions mentioned above as sub-protocols to construct a secure identification protocol.

Finally, we prove that constructing a secure identification protocol non-interactively is impossible, even using oblivious transfer.

Acknowledgements

First of all, I would like to thank my supervisor, Christian Schaffner for introducing me to world of quantum cryptography and for giving me the opportunity to work with him, for his valuable contribution throughout the project, the long hours he spent on trying to solve the riddles of isolated qubits.

Furthermore, I want to thank Yi-Kai Liu for helpful discussions and suggestions as well as reading through our first try to tackle his model.

I would also like to thank the examination committee for taking the time and effort of reading this thesis.

Last but not least, I want to thank my family and friends for their motivation and support during the last year.

Contents

Abstract	i
Acknowledgements	ii
Contents	iii
Abbreviations	vi
1 Introduction	1
1.1 History Of Cryptography: From Art To Science.	1
1.1.1 First Steps: The Art Of Encrypting Messages	1
1.1.2 Modern Cryptography	2
1.1.3 Quantum Cryptography	3
1.2 Secure Two-Party Computation	4
1.2.1 Bit Commitment & Oblivious Transfer	4
1.3 One-Time Memories In The Isolated Qubits Model	5
1.4 Our Contributions	6
1.5 Outline Of The Thesis	6
2 Preliminaries	8
2.1 Basic Notation	8
2.2 Functions	9
2.2.1 Non-Degenerate Linear Functions	9
2.2.2 t -wise Independent Hash Functions	10
2.3 Functionalities & Protocols	10
2.3.1 $\binom{2}{1}$ -OT	11
2.3.2 $\binom{2}{1}$ -ROT	12
2.3.3 $\binom{k}{1}$ -OT	12
2.3.4 $\binom{k}{1}$ -ROT	13
2.3.5 Password-Based Identification	15
2.4 One-Time Memories In The Isolated Qubits Model	16
2.4.1 The Isolated Qubits Model	16
2.4.2 Leaky String $\binom{2}{1}$ -ROT	17
Separable Measurement	18
δ -non-negligible Measurement Outcome	18
2.4.3 Privacy Amplification	18

2.4.4	Comparing The Isolated Qubits And Bounded Quantum Storage Models .	19
3	$\binom{2}{1}$–ROT In The Isolated Qubits Model	20
3.1	Secure String $\binom{2}{1}$ –ROT	20
3.1.1	Protocol String $\binom{2}{1}$ –ROT	20
3.1.2	Security Of The Protocol	21
3.2	Proof Of Theorem 3.3	23
3.2.1	Security For Fixed Measurement M	23
3.2.2	Security For μ –net	26
3.2.3	Approximating Measurement Outcomes	29
4	Flavours Of Oblivious Transfer	36
4.1	$\binom{2}{1}$ –OT from $\binom{2}{1}$ –ROT	36
4.1.1	Proof of Theorem 4.2	37
4.1.1.1	Correctness	37
4.1.1.2	Security for Alice	38
4.1.1.3	Security for Bob	39
4.2	$\binom{k}{1}$ –OT And $\binom{k}{1}$ –ROT From $\binom{2}{1}$ –OT	40
4.3	$\binom{k}{1}$ – $\widetilde{\text{ROT}}$ from $\binom{2}{1}$ –ROT	41
4.3.1	Protocol And Security Definition	41
4.3.2	Proof Of Theorem 4.4	42
4.3.2.1	Correctness	42
4.3.2.2	Security For Alice	43
4.3.2.3	Security For Bob	43
5	Secure Identification	45
5.1	Secure Identification From $\binom{k}{1}$ –OT	45
5.2	Impossibility Proof	46
5.2.1	Non-Interactive Password-Based Identification	46
5.2.2	Proof Of Theorem 5.5	49
	Attack Strategy Of Dishonest User Alice	52
5.2.3	The Importance Of Interaction	52
5.3	Secure Identification From $\binom{k}{1}$ – $\widetilde{\text{ROT}}$ With Interaction	53
5.3.1	Proof Of Theorem 5.10	54
5.3.1.1	Correctness	54
5.3.1.2	Security For Alice	55
5.3.1.3	Security For Bob	56
6	Conclusions & Discussion	58
6.1	Conclusions & Discussion	58
6.2	Future Work	59
A	Probability Theory	61
A.1	Probability Theory	61
A.1.1	Random Variables	61
	Boole’s inequality	62

A.1.2	Uniform Distribution	63
A.1.3	ϵ -Net	63
B	Measures of Uncertainty	64
B.1	Renyi Entropy	64
B.2	Min-Entropy	64
B.3	Smoothed Min-Entropy	65
C	Linear Algebra	66
C.1	Norms	66
	Statistical Distance	66
	Bibliography	67

Abbreviations

OTM	O ne- T ime M emory
OT	O blivious T ransfer
$\binom{2}{1}$ - OT	One-out-of-Two O blivious T ransfer
$\binom{k}{1}$ - OT	One-out-of-k O blivious T ransfer
$\binom{k}{1}$ - ROT	One-out-of-k R andomised O blivious T ransfer
IQM	I solated Q ubits M odel
POVM	P ositive O perator V alued M easurement
LOCC	L ocal O perations and C lassical C ommunication

Chapter 1

Introduction

1.1 History Of Cryptography: From Art To Science.

The word cryptography comes from the greek words $\chi\rho\upsilon\pi\tau\acute{o}$ (“secret”) and $\gamma\rho\acute{\alpha}\varphi\omega$ (“write”). In other words it defines the art of secret message transmission between two parties in a way that the message remains unreadable to any third party (*adversary*). This definition is accurate for the historical uses of cryptography but not for its modern form.

In the last century, cryptography has evolved from art to science that does not rely on the obscurity of the encryption method but on formal mathematical definitions and rigorous security proofs. Furthermore, modern cryptography deals not only with the problem of message encryption but also with problems such as authentication, digital signatures and multi-party computation.

In this section we give a brief overview of the history of cryptography and its evolution from the art of message encryption to its modern forms.

1.1.1 First Steps: The Art Of Encrypting Messages

The practice of cryptography is as old as the transmission of messages. Closely linked to the history of mankind, forms of encryption were developed independently in a number of places and soon again forgotten as were the civilisations that used them.

According to Kahn [Kah96], cryptography has its roots in 1900 BC ancient Egypt, in the use of unusual hieroglyphs, instead of the ordinary ones, in the tomb of a nobleman, Khnumhotep II. Together with the construction of impressive burial monuments, the need to impress the living took the form of decorating tombs with obscure encryptions. These cryptic puzzles did for the first time intend to preserve the secrecy of the original text, at least enough to attract the curiosity of passersby for the short time it would take to decrypt and read.

Although there are probably innumerable examples of these first forms of cryptography we note its first known military use to transmit secret messages, the scytale. First mentioned around the 7th century BC by Apollonius of Rhodes, used by the Spartans the scytale was a method to transmit a message secretly. Plutarch gives a more detailed account of its use in *Lives* (Lysander, 19), two identical wooden rods, the scytalae, are used in the following way. A leather strap is

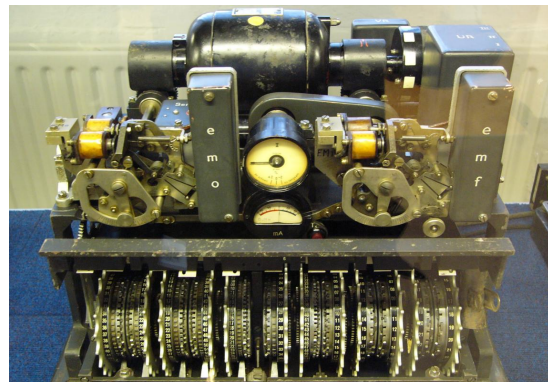
wound around the scytale and then the message is written on it along the length of the rod (see Figure 1.1a). The leather strap is then sent to the receiver of the message who has to wind it around his scytale in order to read the message. If the message is intercepted, it cannot be read unless a rod of the same diameter is used. It is furthermore hypothesized that this could be a method for message authentication instead of encryption, that is only if the sender used the correct scytale is the message readable by the receiver, thus making it more difficult to inject false messages by a third party.

Through the next centuries, the most common use of cryptography was encryption of text through ciphers by substitution of letters in a fixed way such as the Caesar's cipher. The latter uses a fixed left shift of the alphabet by three letters, i.e. A would be transcribed as D, B as E, and so on. More complicated ciphers were developed following the same principle, using a, possibly different, shift of the alphabet for every letter of the message, often defined by a secret key.

The most prominent example of complex substitution ciphers is the use of rotor machines, for example the Enigma and Lorenz cipher machines used in World War II (see Figure 1.1b). These machines used a number of rotating disks (rotors) that implemented a complex, but fixed, substitution of letters. For every keypress the position of the rotors would change thus using a different substitution for every letter.



(A) Scytale



(B) Lorenz rotor stream cipher machine

FIGURE 1.1: Examples of device dependent cryptographic implementations. Figure 1.1a The scytale described in more detail in Section 1.1.1 (Source: <https://commons.wikimedia.org/wiki/File:Skytale.png>) and Figure 1.1b The Lorenz SZ42, an example of a rotor cipher machine (Source: <https://en.wikipedia.org/wiki/File:Lorenz-SZ42-2.jpg>).

1.1.2 Modern Cryptography

For more than twenty centuries cryptography focused mostly on the art of encrypting and conveying secret messages, mainly for military purposes. A large number of very different and sometimes very complex protocols were implemented, but they all relied on the secrecy of the encryption method. Thus once the protocol was known by an adversary it was no longer secure. The beginning of the end of this era of cryptography was foreseen by A. Kerckhoffs in the following statement:

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

A. Kerckhoffs, “La Cryptographie militaire”, 1883

This was later reformulated by C. Shannon as “the enemy knows the system being used” [Sha49], starting the modern era of cryptography, where security of cryptographic schemes or protocols does no longer rely on the obscurity of the encryption methods. For cryptography this was the paradigm shift from art to science.

Modern cryptography relies on the formulation of exact definitions for protocols and rigorous proofs of security¹. Most notably the security of most cryptographic protocols depends on the unproven assumption that some mathematical problems, such as the factorisation of integers², are hard to solve. A problem is computationally hard to solve if there exist no algorithms that can do so in polynomial time. This of course means that these protocols are not indefinitely secure since an adversary would be able to succeed in violating its security given enough time or an algorithm that could solve the problem on which the protocol’s security relies efficiently.

Assumptions about the computational restriction of adversaries have so far proved to be sufficiently strong for modern cryptography, but recent developments in quantum computing showed the existence of an algorithm that can factorise integers in polynomial time if run on a quantum computer, Shor’s algorithm [Sho94]. That means that once sufficiently large quantum computers are in use, the implemented cryptographic protocols will become vulnerable. Faced with this increasingly real danger, cryptographers are trying to develop new approaches to achieve security.

1.1.3 Quantum Cryptography

In the early 1970’s Wiesner proposed the idea of using two-state quantum-mechanical systems, such as polarised photons, to encode and transmit messages [Wie83]. Motivated by Heisenberg’s uncertainty principle he showed that it is possible to use two “conjugate observables”, linear and circular polarisation of photons, to “transmit two messages either but not both of which may be received”. This important result remained unpublished for a decade, but set the basis of a new form of cryptography that no longer relies on the computational limitation of an adversary to achieve security. Quantum cryptography is solely based on the assumption that the laws of quantum mechanics model nature accurately to achieve security.

Although the first steps of quantum cryptography passed almost unnoticed³ Brassard and Bennett used Wiesner’s idea of “conjugate coding” to achieve something previously thought impossible. The quantum key distribution protocol first developed by Bennett and Brassard and later Ekert [BB84, Eke91, BBE92] that allows two users to exchange a secret key over a public quantum communication channel that is eavesdropped on. The strength of this quantum protocol lies in the fact that the users are able to detect an eavesdropper who is trying to obtain their key, since measuring a quantum state disturbs its original state.

Following this important success in quantum cryptography, the horizons of cryptography broadened and the quest to implement more cryptographic tasks such as secure multi-party quantum computation relying on quantum phenomena to achieve security began.

Finally it is important to mention post-quantum cryptography as another approach to face the potential threat of quantum computers for the currently implemented cryptographic protocols.

¹For a detailed introduction we refer to [KL07].

²Integer factorisation is a widely used computational hardness assumption in cryptographic protocols, for example in RSA [RSA78]. So far there exists no algorithm that can solve the problem of factoring a large integer into products of smaller number (usually primes) on a classical computer in polynomial time.

³For a very enjoyable brief account of these first steps refer to [Bra06].

It is the field of search for classical cryptographic assumptions that cannot be broken efficiently by quantum or classical computers [BBD09].

1.2 Secure Two-Party Computation

We have seen that for a long time cryptographers focused on the problem of transmitting secret messages. One further problem of cryptography introduced by Yao in [Yao82] is that of secure multi-party computation. That is the problem where a number of N players each of whom holds an input x_1, \dots, x_N want to evaluate a function of all their inputs, $f(x_1, \dots, x_N)$ correctly without disclosing information about their respective inputs. This is not only an interesting cryptographic problem, but one that leads to a number of useful applications such as secret voting, oblivious negotiation, private querying of database.

While Yao introduced the problem of secure multi-party computation, in [Yao82] he mainly focused on the two-party case. That is the problem of two mutually distrustful parties correctly computing a function without revealing their inputs to each other.

In this thesis we will focus on one problem of two-party computation, namely secure password-based identification: A user Alice identifies herself to a server Bob by securely evaluating the equality function on their inputs (or passwords). In the literature this is often referred to as the “socialist millionaire problem”, a variant of the “millionaire problem”¹, in which the two millionaires want to determine if they are equally rich, without revealing any information about their actual wealth to each other [Yao82].

1.2.1 Bit Commitment & Oblivious Transfer

In this section we focus on two similar but fundamental two-party computation problems, *bit commitment* and *oblivious transfer*, their history and their importance.

Bit commitment schemes consist of two phases, the *commit phase* where the sender Alice chooses the value of a bit and commits to it in the sense that it cannot be changed later and a *reveal phase* during which the hidden value of the bit is revealed and before which the receiver Bob has no information about the value of the bit.

Oblivious transfer is the transfer of information in such a way that the sender does not know what information the receiver obtains. We will give a brief overview of its origin and its importance in secure two-party computation.

The term was coined by Rabin in [Rab81], where he introduced what is now known as Rabin OT, a protocol where one user Alice sends a message and another user Bob does or does not receive it with equal probability, while Alice remains oblivious of the reception of the message, this is often referred to as secure erasure channel.

A similar notion was introduced in the first paper on quantum cryptography “Conjugate Coding”, where Wiesner describes “a means for transmitting two messages, either but not both of which may be received” [Wie83]. This was later rediscovered by Even, Goldreich and Lempel

¹The millionaire or Yao’s millionaire problem is a classic secure multi-party computation problem in which two millionaires want to determine who is richer without disclosing any information about their wealth to each other.

[EGL85] and named *one-out-of-two oblivious transfer* and denoted as $\binom{2}{1}$ -OT. Intuitively it can be thought of as a black box in which a user Alice can store two messages and another user Bob can choose to receive the first or second message but learns no further information about the message he does not receive. Furthermore it fulfills the condition for oblivious transfer, namely that Alice does not know which message Bob received.

A few years later, Crépeau [Cré88] proved that these two flavours of oblivious transfer are equivalent. In the same year Kilian [Kil88] proved that the $\binom{2}{1}$ -OT primitive is complete for two-party computation. This surprising result meant that a secure $\binom{2}{1}$ -OT construction is sufficient to implement any two-party computation, making it a fundamental cryptographic problem. Moreover from the results of [Kil88, Cré88] a $\binom{2}{1}$ -OT protocol can be used to implement bit commitment. Although a classical protocol was already introduced by Even, Goldreich and Lempel [EGL85] it relies on computational assumptions that are insecure against a quantum adversary. After the early success of quantum cryptography, research focused on the problem of constructing unconditionally secure bit commitment schemes [BC91, BCJL93] and oblivious transfer or $\binom{2}{1}$ -OT primitives [BBCS92, Cré94].

Despite these first results, hope to achieve unconditionally secure quantum bit commitment vanished as doing so was proved to be impossible in a quantum setting in [May96, LC97]. As discussed above, since an $\binom{2}{1}$ -OT primitive can be used to implement bit commitment, the impossibility result for bit commitment implies that $\binom{2}{1}$ -OT is also impossible. In [Lo97], Lo proved that all quantum one-sided two-party computations, including $\binom{2}{1}$ -OT are insecure. Furthermore Colbeck in [Col07] and Buhrman et al. in [BCS12] showed that secure two-party computation is impossible to achieve in a fully quantum setting.

One way to circumvent these impossibility results is to impose realistic restrictions on the users. In the literature there are two successful models that do so, the bounded-quantum-storage model [DFSS07, DFSS08] that upper bounds the size of quantum memory of the users and the noisy-storage model [WST08, KWW12, Sch10] that assumes that the quantum memory used is imperfect. Under the assumption of bounding the quantum storage of a user, unconditionally secure oblivious transfer, $\binom{2}{1}$ -OT and thus two-party computation can be achieved [DFSS07, DFSS08].

1.3 One-Time Memories In The Isolated Qubits Model

In 2013 Liu [Liu14a] suggested a further alternative to the memory-restricting models discussed in the previous section, the *isolated qubits model*, where all parties are restricted to the use of *local operations* on each qubit and *classical communication* (LOCC). The restriction to local quantum operations on each qubit means that the users are not allowed to perform entangling operations on the isolated qubits. The model is motivated by experimental work on nitrogen vacancy centers in diamond that can be read out and manipulated optically while at the same time it is difficult to perform entangling operations on pairs of such centers. We discuss the isolated qubits model in more detail in Chapter 2.

A *one-time memory* (OTM) is a protocol or cryptographic device in which Alice stores two messages and sends it to Bob, who is then able to retrieve only one of the two messages. In essence it is a non-interactive or one-way $\binom{2}{1}$ -OT, but we will discuss their difference in more detail in Section 2.4.2 Liu showed that it is possible to build an imperfect OTM in the IQM that leaks a fraction of information about the unreceived message [Liu14a, Liu14b]. Furthermore,

Liu recently showed that it is possible to use privacy amplification in order to achieve a secure OTM for a single bit [Liu15].

A significant difference between the isolated qubits model and the noisy- and bounded-quantum-storage models is that the parties are not forced to measure the qubits soon after reception, rather they are allowed to store the qubits for an indefinite amount of time. This means that the users are allowed to take advantage of any further information shared between them at a later point to decide on their measurement strategy. On the other hand the noisy- and bounded-quantum-storage models allow entangling operations between the users which is not allowed in the isolated qubits model. In this sense the memory-restricting and isolated qubits models are complementary, which is reflected in the fact that protocols that are secure in one model are not secure in the other. Protocols in the noisy- or bounded-quantum-storage model are insecure in the isolated qubits model in which the adversary has access to unlimited and perfect storage of isolated qubits. The opposite is also true since the protocol presented in [Liu14b] is not secure against an adversary that can perform entangling operations. We will discuss this in more detail in Section 2.4.4.

1.4 Our Contributions

In this thesis, we study the constructions of “leaky” string and secure single-bit one-time memories in the isolated qubits model (IQM) introduced in [Liu14a, Liu14b, Liu15]. Using non-linear degenerate functions [DFSS06] we simplify the proof presented in [Liu15]. We then construct and prove the security of a string *one-out-of-two sender-randomised oblivious transfer*, $\binom{2}{1}$ -ROT, protocol in this model.

Relying on the construction of a secure string $\binom{2}{1}$ -ROT protocol we study for the first time interactive protocols for more complex two-party functionalities in the IQM. In order to do so, we assume that all parties measure the qubits they receive at the end of each sub-protocol, which allows us to construct composed protocols. First, we construct a $\binom{2}{1}$ -OT protocol that makes use of one instance of a $\binom{2}{1}$ -ROT functionality and prove its security. We then construct a weak but efficient *sender-randomised one-out-of-k oblivious transfer*, $\binom{k}{1}$ - $\widetilde{\text{ROT}}$, protocol. Finally, we construct a protocol that implements the password-based identification functionality securely, relying on a secure $\binom{k}{1}$ - $\widetilde{\text{ROT}}$.

Moreover, we study the possibility to construct protocols that implement the password-based identification functionality securely and non-interactively. We prove that such an implementation is impossible relying only on one-way transmission or even oblivious transfer of messages and qubits from Alice to Bob.

1.5 Outline Of The Thesis

In Chapter 2, we introduce notation, the basic concepts from cryptography as well as the model we use in this thesis. In Chapter 3, we extend bit one-time memories introduced in [Liu14a, Liu14b, Liu15] to string $\binom{2}{1}$ -ROTs using results from [DFSS06]. In Chapter 4, we study more complex two-party functionalities that make use of multiple instances of the $\binom{2}{1}$ -ROTs constructed in Chapter 3. Firstly, we construct a $\binom{2}{1}$ -OT protocol that makes use of one $\binom{2}{1}$ -ROT functionality. Secondly, we study a $\binom{k}{1}$ -OT protocol presented in [BCR86] that

makes use of $k \binom{2}{1}$ -OTs. Finally, we present a construction for a weaker but more efficient $\binom{k}{1} - \widetilde{\text{ROT}}$ protocol that uses only $\log k \binom{2}{1}$ -ROTs. In Chapter 5, we prove that constructing a non-interactive identification protocol is impossible even using secure $\binom{k}{1}$ -OT functionalities. We then propose a protocol to achieve secure password-based identification and prove its security using the secure $\binom{k}{1} - \widetilde{\text{ROT}}$ constructed in Chapter 4. In the last Chapter 6 we summarise our results and discuss their significance.

Chapter 2

Preliminaries

In this chapter, we introduce notation and the basic tools that we will use in this thesis.

We assume some familiarity with basic probability theory and quantum information theory. A brief overview of the probability theory notions used in this thesis can be found in [Appendix A](#) and for an indepth introduction to quantum information theory we refer the reader to [\[NC00\]](#).

2.1 Basic Notation

We use uppercase letters such as X, Y, Z to denote random variables, calligraphic letters $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ to denote sets and lowercase letters x, y, z to denote a specific value of a random variable. Furthermore, for a sequence of random variables X_1, \dots, X_k we write \overline{X}_i , with $i \in \{1, \dots, k\}$ to denote the sequence X_1, \dots, X_k excluding X_i .

Moreover, we introduce the symbol $P_{X \leftrightarrow Y \leftrightarrow Z}$, as used in [\[DFSS07\]](#) and [\[FS09\]](#), to denote that the distribution of a random variable X is independent of a random variable Z given a random variable Y :

$$P_{X|YZ} = P_{X|Y}, \quad (2.1)$$

we then write:

$$P_{XYZ} = P_{X \leftrightarrow Y \leftrightarrow Z}. \quad (2.2)$$

This notation is extended to $P_{XYZ|\mathcal{E}} = P_{X \leftrightarrow Y \leftrightarrow Z|\mathcal{E}}$ to denote that the distribution of a random variable X is independent of a random variable Z given a random variable Y conditioned on an event \mathcal{E} :

$$P_{X|YZ\mathcal{E}} = P_{X|Y\mathcal{E}}. \quad (2.3)$$

Finally, the *smoothed min-entropy* of a random variable X conditioned on a random variable Y is denoted by $H_\infty^\varepsilon(X|Y)$. For more information we refer the reader to Appendix B.

For any matrix $A \in \mathbb{C}^{m \times n}$ and vector $x \in \mathbb{C}^n$ we use $\|A\|$, $\|A\|_F$ and $\|A\|_{\text{tr}}$ to denote the operator, the Frobenius and the trace norm respectively. Further information on these norms is included in Appendix C.

A brief overview of the Bachmann-Landau symbols:

We write $f(k) = O(g(k))$ if $\exists c > 0, \exists k_0, \forall k > k_0 : |f(k)| \leq c|g(k)|$.

We write $f(k) = o(g(k))$ if $\forall c > 0, \exists k_0, \forall k > k_0 : |f(k)| \leq c|g(k)|$.

We write $f(k) = \Omega(g(k))$ if $\exists c > 0, \exists k_0, \forall k > k_0 : |f(k)| \geq c|g(k)|$.

We write $f(k) = \Theta(g(k))$ if $\exists c_1 > 0, \exists c_2 > 0, \exists k_0, \forall k > k_0 : c_1|g(k)| \leq |f(k)| \leq c_2|g(k)|$.

2.2 Functions

In this section we give a brief overview of special families of functions that we use in this thesis:

2.2.1 Non-Degenerate Linear Functions

Non-degenerate linear functions are functions that depend non-trivially on their inputs and are defined in [DFSS06, Definition 4.2] as follows:

Definition 2.1. *A function $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \mapsto \{0,1\}$ is called a non-degenerate linear function if it is of the form:*

$$\beta : (s_0, s_1) \mapsto \langle u_0, s_0 \rangle \oplus \langle u_1, s_1 \rangle \quad (2.4)$$

for two non-zero strings $u_0, u_1 \in \{0,1\}^\ell$, where $\langle \cdot, \cdot \rangle$ is the bit-wise inner product defined as:

$$\langle a, b \rangle = \bigoplus_{i=1}^{\ell} a_i \cdot b_i \quad (2.5)$$

We further mention the definition of a more relaxed notion.

Definition 2.2. [DFSS06, Definition 4.3] *A binary function $\beta : \{0,1\}^\ell \times \{0,1\}^\ell \mapsto \{0,1\}$ is called 2-balanced if for any $s_0, s_1 \in \{0,1\}^\ell$ the functions $\beta(s_0, \cdot)$ and $\beta(\cdot, s_1)$ are balanced, meaning that $|\{\sigma_1 \in \{0,1\}^\ell : \beta(s_0, \sigma_1) = 0\}| = 2^\ell/2$ and $|\{\sigma_0 \in \{0,1\}^\ell : \beta(\sigma_0, s_1) = 0\}| = 2^\ell/2$.*

Finally we note the following result that will allow us to use the fact that for any string s_i the functions $\beta(s_i, \cdot)$ and $\beta(\cdot, s_i)$ are balanced in the proof of Lemma 3.6 in Section 3.2.1

Lemma 2.3. [DFSS06, Lemma 4.4] *Every non-degenerate linear function is 2-balanced.*

2.2.2 t -wise Independent Hash Functions

We introduce the definition of t -wise independent hash functions as defined in [Liu15].

Definition 2.4. Let \mathcal{H} be a family of functions $h : \{1, \dots, N\} \mapsto \{1, \dots, M\}$ and H be a function chosen uniformly at random from \mathcal{H} . We call \mathcal{H} a family of t -wise independent functions if for all subsets $S \subset \{1, \dots, N\}$ of size $|S| \leq t$, where $t \geq 1$ is an integer, the random variables $\{H(x) | x \in S\}$ are independent and uniformly distributed in $\{1, \dots, M\}$.

Note that sampling and applying a random function from a family of t -wise independent hash functions can be done efficiently ([Liu15, Proposition 2.5]).

We present a large-deviation bound for quadratic functions of $2t$ -wise independent random variables [Liu15, Proposition 2.7]:

Proposition 2.5. Let $t \geq 2$ be an even integer, and let \mathcal{H} be a family of $2t$ -wise independent functions $\{1, \dots, N\} \mapsto \{0, 1\}$. Let $A \in \mathbb{R}^{N \times N}$ be a symmetric matrix, $A^T = A$. Let H be a function chosen uniformly at random from \mathcal{H} , and define the random variable

$$S = \sum_{x,y=1}^N A_{xy} \left((-1)^{H(x)} (-1)^{H(y)} - \delta_{xy} \right), \quad (2.6)$$

where δ_{xy} is the Kronecker δ that equals 1 if $x = y$ and 0 otherwise.

Then the expected value of S is $\mathbb{E}[S] = 0$ and we have the following large-deviation bound: for any $\lambda > 0$,

$$P(|S| \geq \lambda) \leq 4e^{\frac{1}{6t}} \sqrt{\pi t} \left(\frac{4\|\tilde{A}\|_F^2 t}{e\lambda^2} \right)^{\frac{t}{2}} + 4e^{\frac{1}{12t}} \sqrt{2\pi t} \left(\frac{8\|\tilde{A}\|^2 t}{e\lambda} \right)^t, \quad (2.7)$$

where $\tilde{A} \in \mathbb{R}^{N \times N}$ is the entry-wise absolute value of A , that is $\tilde{A}_{xy} = |A_{xy}|$.

2.3 Functionalities & Protocols

An ideal functionality formally describes a cryptographic task, detailing the behaviours of honest and dishonest parties. A protocol is a series of clearly defined instructions that the (honest) parties follow. Finally we define the security for a protocol, describing the conditions that need to be fulfilled in order for a protocol to implement a functionality securely.

In this section, we introduce the ideal functionalities of $\binom{2}{1}$ -OT, $\binom{2}{1}$ -ROT, $\binom{k}{1}$ -OT, $\binom{k}{1}$ -ROT, $\binom{k}{1}$ - $\widetilde{\text{ROT}}$ and password-based identification as well as equivalent security definitions that we will use in the following chapters.

2.3.1 $\binom{2}{1}$ -OT

First, we formally define the $\binom{2}{1}$ -OT functionality, that we discussed in Chapter 1, that allows two parties to share one out of two messages such that the sender is oblivious as to which message has been received, while the receiver has no knowledge of the second message.

Functionality 2.6. Upon receiving input messages $A_0, A_1 \in \mathcal{X}$ from Alice, where $\mathcal{A} = \{0, 1\}^l$ and the choice bit $D \in \{0, 1\}$ from Bob, $\mathcal{F}_{\binom{2}{1}\text{-OT}}$ outputs A_D to Bob and outputs nothing to Alice.

Commonly security of a protocol is proven by showing that a real protocol is indistinguishable from the ideal functionality. However there exists an alternative approach, [FS09, Proposition 4.3] allows us to use an equivalent security definition. If a protocol fulfills this definition, then it securely implements the ideal functionality.

Definition 2.7. A ε -secure $\binom{2}{1}$ -OT protocol is a protocol between Alice with inputs $A_0, A_1 \in \mathcal{A}$ and Bob with input $D \in \{0, 1\}$ such that the following holds:

Correctness: For honest user Alice and honest server Bob, for any distribution of Alice's inputs $A_0, A_1 \in \mathcal{A}$ and Bob's input $D \in \{0, 1\}$, Alice gets no output and Bob receives output $G = A_D$, except with probability ε .

Security for Alice: For any dishonest server Bob with output G' , there exists a random variable $D' \in \{0, 1\}$ such that:

$$P_{D'A_0A_1} \approx_\varepsilon P_{D'} \cdot P_{A_0A_1} \quad (2.8)$$

and

$$P_{G'A_{D'}D'A_{1-D'}} \approx_\varepsilon P_{G'|A_{D'}D'} \cdot P_{A_{D'}D'A_{1-D'}} \quad (2.9)$$

Security for Bob: For any dishonest user Alice with output V' , there exists random variables A'_0, A'_1 such that:

$$P[G = A'_D] \geq 1 - \varepsilon, \quad (2.10)$$

and

$$P_{DV'A'_0A'_1} \approx_\varepsilon P_D \cdot P_{V'A'_0A'_1} \quad (2.11)$$

2.3.2 $\binom{2}{1}$ -ROT

While $\binom{2}{1}$ -OT is a powerful tool we present a different oblivious transfer functionality, the randomised one-out-of-two oblivious transfer $\binom{2}{1}$ -ROT. Contrary to the $\binom{2}{1}$ -OT Alice does not input two messages but receives two random messages from the functionality while Bob receives one out of the two messages depending on his input choice. We present the formal definition of the $\binom{2}{1}$ -ROT functionality.

Functionality 2.8. Upon receiving no input from Alice and the choice bit $D \in \{0, 1\}$ from Bob, $\mathcal{F}_{\binom{2}{1}\text{-ROT}}$ outputs messages $A_0, A_1 \in \mathcal{A}$, where $\mathcal{A} = \{0, 1\}^\ell$ to Alice and message A_D to Bob.

Furthermore, we introduce an equivalent security definition that protocols that securely implement the $\binom{2}{1}$ -ROT functionality should fulfill.

Definition 2.9. A ε -secure $\binom{2}{1}$ -ROT protocol is a protocol between Alice with no input and Bob with input $D \in \{0, 1\}$ such that the following holds:

Correctness: For honest user Alice and honest server Bob, for any distribution of Bob's input $D \in \{0, 1\}$, Alice receives output $A_0, A_1 \in \mathcal{A}$ and Bob receives output $G = A_D$, except with probability ε .

Security for Alice: For any dishonest server Bob with output G , there exists a random variable $D' \in \{0, 1\}$ such that:

$$P_{A_1-D'GA_{D'}D'} \approx_\varepsilon P_U \cdot P_{GA_{D'}D'} \quad (2.12)$$

Security for Bob: For any dishonest user Alice with output V' , there exists random variables A'_0, A'_1 such that:

$$P[G = A'_D] \geq 1 - \varepsilon, \quad (2.13)$$

and

$$P_{DV'A'_0A'_1} \approx_\varepsilon P_D \cdot P_{V'A'_0A'_1} \quad (2.14)$$

2.3.3 $\binom{k}{1}$ -OT

In this section, we focus on a generalised oblivious transfer functionality that takes k inputs instead of two, the 1-out-of- k Oblivious Transfer, denoted as $\binom{k}{1}$ -OT. It is a two-party functionality between a user Alice that inputs k messages X_1, X_2, \dots, X_k and a user Bob who is allowed to retrieve only one of these messages X_D according to his choice D . When the above functionality is implemented securely, Bob should not be able to learn additional information

on any of the other messages. At the same time, the obliviousness of the protocol must still hold, Alice should not have any knowledge about the choice of Bob.

The formal definition of the $\binom{k}{1}$ -OT functionality is the following:

Functionality 2.10. Upon receiving input messages $X_1, \dots, X_k \in \mathcal{X}$ from Alice, where $\mathcal{X} = \{0, 1\}^l$ and the choice $D \in \{1, \dots, k\}$ of Bob, $\mathcal{F}_{\binom{k}{1}\text{-OT}}$ outputs X_D to Bob and outputs nothing to Alice.

We now introduce an equivalent security definition for the $\binom{k}{1}$ -OT functionality.

Definition 2.11. A ε -secure $\binom{k}{1}$ -OT protocol is a protocol between Alice with inputs $X_1, \dots, X_k \in \mathcal{X}$ and Bob with input $D \in \{1, \dots, k\}$ such that the following holds:

Correctness: For honest user Alice and honest server Bob, for any distribution of Alice's inputs $X_1, \dots, X_k \in \mathcal{X}$ and Bob's input $D \in \{1, \dots, k\}$, Alice gets no output and Bob receives output $G = X_D$, except with probability ε .

Security for Alice: For any dishonest server Bob with output G' , there exists a random variable $D' \in \{1, \dots, k\}$ such that:

$$P_{D'X_1\dots X_k} \approx_\varepsilon P_{D'} \cdot P_{X_1\dots X_k} \quad (2.15)$$

and

$$P_{G'X_{D'}D'\overline{X_{D'}}} \approx_\varepsilon P_{G'|X_{D'}D'} \cdot P_{X_{D'}D'\overline{X_{D'}}} \quad (2.16)$$

Security for Bob: For any dishonest user Alice with output V' , there exist random variables X'_1, \dots, X'_k such that:

$$P[G = X'_D] \geq 1 - \varepsilon, \quad (2.17)$$

and

$$P_{DV'X'_1\dots X'_k} \approx_\varepsilon P_D \cdot P_{V'X'_1\dots X'_k} \quad (2.18)$$

2.3.4 $\binom{k}{1}$ -ROT

In this section we introduce a slightly different flavour of the $\binom{k}{1}$ -OT, where the user Alice does not input messages X_1, \dots, X_k but instead has no inputs and receives as output k random messages S_1, \dots, S_k . This functionality is defined formally below:

Functionality 2.12. *Honestly behaving Alice and Bob: Upon receiving no input from Alice and a choice $D \in \{1, \dots, k\}$ from Bob, $\mathcal{F}_{(1)}^{(k)}\text{-ROT}$ samples random independent strings $S_1, \dots, S_k \in \mathcal{S} = \{0, 1\}^\ell$ and sends S_1, \dots, S_k to Alice and S_D to Bob.*

Honest Alice and dishonest Bob: Upon receiving no input from Alice, a choice $D \in \{1, \dots, k\}$ and a string $S_D \in \mathcal{S}$ from Bob, $\mathcal{F}_{(1)}^{(k)}\text{-ROT}$ samples random independent strings $\overline{S_D} \in \mathcal{S}$, and sends S_1, \dots, S_k to Alice.

Dishonest Alice and honest Bob: Upon receiving input messages $S_1, \dots, S_k \in \mathcal{S}$ from Alice, where \mathcal{S} and the choice $D \in \{1, \dots, k\}$ of Bob, $\mathcal{F}_{(1)}^{(k)}\text{-ROT}$ outputs S_D to Bob and outputs nothing to Alice.

We introduce the security definition for the $(\binom{k}{1})\text{-ROT}$ functionality.

Definition 2.13. *The sender-randomised $(\binom{k}{1})\text{-ROT}$ is secure if the following conditions are fulfilled:*

Correctness: *For honest user Alice and honest server Bob, for any distribution of Bob's input D , Alice gets outputs $S_1, \dots, S_k \in \mathcal{S}$ uniform and independent of D and Bob receives output S_D , except with probability ε .*

Security for Alice: *For any dishonest server Bob with output G' , there exists a random variable $D' \in \{1, \dots, k\}$ such that:*

$$P_{\overline{S_{D'}}, S_{D'}, D', G'} \approx_\varepsilon P_{U^{k-1}} \cdot P_{S_{D'}, D', G'} \quad (2.19)$$

Security for Bob: *For any dishonest user Alice with output V' , there exist random variables S'_1, \dots, S'_k such that:*

$$P[G = S'_D] \geq 1 - \varepsilon, \quad (2.20)$$

and

$$P_{DV', S'_1, \dots, S'_k} \approx_\varepsilon P_D \cdot P_{V', S'_1, \dots, S'_k} \quad (2.21)$$

Finally we introduce the security definition for a slightly weaker $(\binom{k}{1})\text{-ROT}$ functionality that we call $(\binom{k}{1})\text{-}\widetilde{\text{ROT}}$.

Definition 2.14. *The sender-randomised $(\binom{k}{1})\text{-}\widetilde{\text{ROT}}$ is ε -secure if the following conditions are fulfilled:*

Correctness: *For honest user Alice and honest server Bob, for any distribution of Bob's input D , Alice gets outputs $S_1, \dots, S_k \in \mathcal{S}$ uniform and independent of D and Bob receives output S_D , except with probability ε .*

Security for Alice: For any dishonest server Bob with output G' , there exists a random variable $D' \in \{1, \dots, k\}$ such that for all $I \neq D'$:

$$P_{S_I S_{D'} D' G'} \approx_\varepsilon P_U \cdot P_{S_{D'} D' G'} \quad (2.22)$$

Security for Bob: For any dishonest user Alice with output V , there exist random variables S'_1, \dots, S'_k such that:

$$P[G = S'_D] \geq 1 - \varepsilon, \quad (2.23)$$

and

$$P_{DV' S'_1, \dots, S'_k} \approx_\varepsilon P_D \cdot P_{V' S'_1, \dots, S'_k} \quad (2.24)$$

The $\binom{k}{1} - \widetilde{\text{ROT}}$ is weaker since although every message that does not correspond to Bob's input remains hidden, this is not true for all messages simultaneously. While weaker, the $\binom{k}{1} - \widetilde{\text{ROT}}$ functionality is strong enough to construct a secure password-based identification protocol as we will show in Chapter 5. Furthermore the $\binom{k}{1} - \widetilde{\text{ROT}}$ protocol we present in Chapter 4 is more efficient than the $\binom{k}{1} - \text{ROT}$ and $\binom{k}{1} - \text{OT}$ protocols, as it makes use of $\log k$ instead of k $\binom{2}{1} - \text{OTs}$.

2.3.5 Password-Based Identification

We define the functionality of identification, where a user Alice identifies herself to a server Bob by securely evaluating the equality function on their inputs, called passwords. Our definition is motivated by [FS09].

Functionality 2.15. Upon receiving strings $W_A \in \mathcal{W}$ from user Alice, where $\mathcal{W} := \{1, \dots, k\}$, and $W_B \in \mathcal{W}$ from server Bob, \mathcal{F}_{ID} outputs the bit $G = W_A \stackrel{?}{=} W_B$ to Bob. In case Alice is dishonest she may choose $W_A = \perp$ (which never agrees with honest Bob's input) and (for any choice of W_A) the bit G is also output to Alice.

The idea behind the \mathcal{F}_{ID} functionality is that Alice and Bob both have an input string W_A and W_B respectively to act as a password and Bob receives and outputs a bit corresponding to the acceptance of Alice's password if their chosen inputs are the same or the rejection if their inputs are not equal. In order for a protocol that fulfills the \mathcal{F}_{ID} functionality to be secure, a dishonest server should not be able to learn Alice's password, except with the probability that he guesses the password correctly. At the same time it has to be secure against a dishonest user Alice, so that Bob will not accept her password if it does not correspond to his choice W_B . We introduce the definition that should be fulfilled by secure password-based identification protocols.

Definition 2.16. A password-based identification protocol is ε -secure if the following conditions are fulfilled:

Correctness: For honest user Alice and honest server Bob with inputs $W_A = W_B$, Bob outputs $G = 1$ except with probability ε .

Security for Alice: For any dishonest server Bob with output G' , for any distribution of W_A , there exists a random variable W' that is independent of W_A such that :

$$P_{W_A W' G' | W' \neq W_A} \approx_\varepsilon P_{W_A \leftrightarrow W' \leftrightarrow G' | W' \neq W_A}. \quad (2.25)$$

Security for Bob: For any dishonest user Alice with output V' , for any distribution of W_B , there exists a random variable W' independent of W_B such that if $W' \neq W_B$ then $P[G = 1] \leq \varepsilon$ and :

$$P_{W_B W' V' | W' \neq W_B} \approx_\varepsilon P_{W_B \leftrightarrow W' \leftrightarrow V' | W' \neq W_B}. \quad (2.26)$$

2.4 One-Time Memories In The Isolated Qubits Model

2.4.1 The Isolated Qubits Model

In Chapter 1, we gave a brief introduction of the isolated qubits model that was first presented by Liu in [Liu14a]. In more detail, parties in this model are restricted to local quantum operations on each qubit and classical communication between the qubits. As detailed in [Liu14a] any local operation and classical communication (LOCC) strategy, in the sense described above, can be described by a series of adaptive single-qubit measurements. In subsequent work, Liu describes how to model any LOCC adversary by a separable positive-operator-value measurement (POVM) [Liu14b].

Furthermore, in contrast with the memory-restricting models described in Chapter 1, in the isolated qubits model, all parties are allowed to store qubits for a long time and are not allowed to perform entangling operations between qubits. While the restriction on entanglement operations reduces the power of an adversary, the possibility to store qubits for a long time has some important implications. An adversary is thus allowed to store qubits and measure them at the end of a protocol, making use of any information he receives to decide on his measurement strategy. Thus usual privacy amplification techniques using hash functions are not effective, which necessitates the use of stronger families of hash functions and a different approach on using them, as described in [Liu15]. We will describe this in more detail in Section 2.4.3.

Moreover the ability of storing qubits for a long time allows an adversary to measure the qubits received at the end of the composed protocol¹.

It is then not clear if the sub-protocols remains secure. Composability in the isolated qubits model has not been studied and it seems to be a non-trivial problem.

¹In cryptography, it is common usage to make calls to secure functionalities in a protocol. For example one could use a series of n single-bit commitment functionalities to commit to an n -bit string. One then argues that since every single bit is committed securely, the same holds for the concatenation of these bits. Composability of protocols allows one to use a modular design to construct and prove the security of complex protocols.

In this thesis we assume that all parties have to measure all qubits used in a sub-protocol at the latest at the end of this sub-protocol. This rather strong assumption allows us to construct composed protocols that make calls to functionalities as sub-routines.

2.4.2 Leaky String $\binom{2}{1}$ –ROT

In this section, we introduce a protocol for imperfect $\binom{2}{1}$ –ROT motivated by the “leaky” one-time memory (OTM) construction presented in [Liu14b].

The security definitions for the “leaky” and perfect OTMs presented in [Liu14b, Liu15] are similar to the $\binom{2}{1}$ –ROT security definition, introduced earlier in this chapter. In Chapter 3 we use the “leaky” $\binom{2}{1}$ –ROT presented here to construct protocols a secure string $\binom{2}{1}$ –ROT. We then use the latter in Chapter 4 to construct a secure $\binom{2}{1}$ –OT protocol.

For consistency with the view of cryptographic tasks as functionalities that are implemented by protocols we do not use the notion of one-time memories as devices that store two messages out of which only one can be read. We instead construct protocols that implement the $\binom{2}{1}$ –ROT functionality (Functionality 2.8) between two users, Alice and Bob. The main difference between an OTM and an oblivious transfer protocol is the fact that the first is non-interactive in the sense that only Alice sends information to Bob, while an oblivious transfer protocol is not necessarily non-interactive. In that sense, the latter is weaker since an OTM implements the oblivious transfer functionality, but an interactive oblivious transfer protocol does not implement the OTM functionality.

We first rewrite the “leaky” OTM as introduced in [Liu14b] as a non-interactive “leaky” $\binom{2}{1}$ –ROT protocol that takes no input from Alice and input D from Bob, and outputs s and t to Alice and one of the two messages to Bob depending on his input choice. This protocol leaks some information about both messages to Bob and is thus not secure.

Protocol 2.17. *A protocol for “leaky” string $\binom{2}{1}$ –ROT between users Alice with no input and Bob with input $D \in \{0, 1\}$ respectively.*

Let $C' : \{0, 1\}^\ell \mapsto \{0, 1\}^{n \log q}$ be an error correcting code that is linear in $GF(2)$ and approaches the capacity of a q -ary symmetric channel \mathcal{E}_q with error probability $p_e = \frac{1}{2} - \frac{1}{2q}$.

1. *Alice samples and receives as output two strings $s, t \in \{0, 1\}^\ell$ uniformly at random.*
2. *Alice computes $C'(s)$ and $C'(t)$ and views them as n blocks of $\log q$ qubits.*
3. *Alice prepares the qubits in the following way and sends them to Bob:*
For $i = 1, \dots, n$:
 - (a) *Let $\gamma_i \in \{0, 1\}$ be the outcome of an independent and fair coin toss.*
 - (b) *If $\gamma_i = 0$ then prepare the i^{th} block of $\log q$ qubits of the codeword $C'(s)$ in the computational basis: $|C'(s)_i\rangle$*
 - (c) *If $\gamma_i = 1$ then prepare the i^{th} block of $\log q$ qubits of the codeword $C'(t)$ in the computational basis: $H^{\otimes \log q} |C'(t)_i\rangle$*
4. *Bob measures every qubit in the base corresponding to his input $D \in \{0, 1\}$ in the following way:*

- If $D = 0$, he measures all the qubits he receives in the computational basis.
 - If $D = 1$, he measures all the qubits he receives in the Hadamard basis.
5. Bob runs the decoding algorithm for C' on the string of measurement outcomes $z \in \{0, 1\}^{n \log q}$ and receives s or t depending on his choice D .

We present the definitions for separable measurements and δ -non-negligible measurement outcomes as presented in [Liu14b], that are used in Theorem 2.19 and later in Chapter 3.

Separable Measurement A measurement on m qubits is called *separable* if it can be written in the form $\mathcal{E} : \rho \mapsto \sum_i K_i^\dagger \rho K_i$, where each operator K_i is a tensor product of m single-qubit operators $K_i = K_{i,1} \otimes \cdots \otimes K_{i,m}$

δ -non-negligible Measurement Outcome

Definition 2.18. For any quantum state $\rho \in \mathbb{C}^{d \times d}$, and any $\delta > 0$, we say that a measurement outcome (POVM element) $M \in \mathbb{C}^{d \times d}$ is δ -non-negligible if $\text{tr}(M\rho) \geq \delta \cdot \text{tr}(M)/d$.

We rephrase the main result of the original paper, [Liu14b, Theorem 2.3], that defines the security of the protocol:

Theorem 2.19 (“Leaky” String $\binom{2}{1}$ –ROT). For any $k \geq 2$, and for any small constant $0 < \mu \ll 1$, Protocol 2.17 between Alice with no input and Bob with input $D \in \{0, 1\}$, has the following properties:

1. *Correctness:* For honest users Alice and Bob, Alice receives two messages $s, t \in \{0, 1\}^\ell$, where $\ell = \Theta(k^2)$ and Bob receives either s or t depending on his choice D , using only LOCC operations.
2. *“Leaky” security:* Let $\delta_0 > 0$ be any constant, and set $\delta = 2^{-\delta_0 k}$. Honest user Alice receives outputs $s, t \in \{0, 1\}^\ell$. For any dishonest LOCC Bob, and any separable measurement outcome M that is δ -non-negligible, we have the following security bound:

$$H_\infty^\varepsilon(S, T | Z = M) \geq \left(\frac{1}{2} - \mu\right) \ell - \delta_0 k. \quad (2.27)$$

Here S and T are the random variables describing the two messages, Z is the random variable representing the Bob’s measurement outcome, and we have $\varepsilon \leq e^{-\Omega(k)}$.

The proof of this theorem can be found in [Liu14b]. This $\binom{2}{1}$ –ROT protocol leaks a constant fraction of information to Bob and is thus not secure for cryptographic tasks.

2.4.3 Privacy Amplification

Common privacy amplification techniques rely on applying a function with a random seed to the string the user holds and require the users to share their seed at a later point. These techniques cannot be used in the isolated qubits model as a dishonest user can postpone his measurement until he has knowledge of the seed and use that information to adapt his measurement.

Liu introduces a privacy amplification technique that can be used in the isolated qubits model in [Liu15]. The technique relies on the use of a fixed hash function of a family of r -wise hash functions, that is a family of stronger hash functions than the ones described above. This method allows privacy amplification on the output of a leaky string OTM as the ones presented in [Liu14a, Liu14b] and leads to the construction of a secure single-bit OTM [Liu15]. In Chapter 3 we follow a similar approach to achieve secure string $\binom{2}{1}$ -ROT, instead of the single-bit OTM presented in [Liu15].

2.4.4 Comparing The Isolated Qubits And Bounded Quantum Storage Models

In Section 1.3 we mentioned briefly that the OTM protocols studied in [Liu14a, Liu14b, Liu15] are not necessarily secure in the noisy- and bounded-quantum-storage models and that at the same time protocols that rely on a quantum memory bound to achieve security are not guaranteed to be secure in the isolated qubits model.

In more detail, the OTM protocols constructed in the isolated qubits model are insecure in a model where entangling operations are allowed. An attack against the OTM protocols by an adversary who is allowed to perform entangling operations has been sketched in [Liu14b], relying on the gentle measurement lemma [Win99] and running the decoding algorithm for the error-correcting code on a superposition of many different inputs. This implies that the OTM and $\binom{2}{1}$ -ROT protocols described in [Liu14a, Liu14b, Liu15] and this thesis are not secure in the noisy- and bounded-quantum-storage models.

On the other hand protocols in the noisy- and bounded-quantum-storage model [WST08, KWW12, Sch10], rely on the memory bound or imperfect storage in order to achieve security. In protocols such as Protocol 5.1, one user encodes qubits in the computational or Hadamard basis while the receiver measures the qubits either in a random basis or in a sequence of bases depending on his input. Since these measurements are destructive, the users commit to a particular choice of measurement bases. The correct sequence of bases is announced between the users at a later point, after the memory-bound has been applied. This step allows the users to know which qubits they have measured in the same basis and thus have obtained the same result, unless the quantum communication channel is being eavesdropped on. At the same time the step of announcing the bases used to encode the sent qubits can be exploited by a malicious user in the isolated qubits model. Since the users are allowed to store the received qubits for an indefinite amount of time after receiving the qubits, an adversary is allowed to wait until he has received the sequence of bases and thus measure all qubits correctly, which violates the security of these protocols.

Thus we argue that protocols that rely on the restriction of a user to perform non-entangling operations cannot be secure in the memory restricting models. On the other hand protocols that rely on the inability of an adversary to store qubits noiselessly or in large numbers cannot be secure in the isolated qubits model.

Chapter 3

$\binom{2}{1}$ –ROT In The Isolated Qubits Model

In this chapter, we introduce a $\binom{2}{1}$ –ROT protocol in the isolated qubits model (IQM), motivated by the “ideal” OTM presented in [Liu15]. Our protocol takes no input from Alice and one bit D as Bob’s input, and outputs two strings A_0 and A_1 to Alice and one string A_D to Bob. This protocol first uses the “leaky” $\binom{2}{1}$ –ROT protocol presented in Chapter 2 and makes use of the privacy amplification technique introduced in [Liu15] to achieve security. The $\binom{2}{1}$ –ROT protocol differs from the “ideal” OTM of [Liu15] in the fact that the messages are strings instead of single bits as in the original. To prove the security of the $\binom{2}{1}$ –ROT protocol we use some results presented in [DFSS06] that allow us to simplify and extend the proof to longer messages, a technique that was not used in the original.

3.1 Secure String $\binom{2}{1}$ –ROT

As discussed in the previous chapter, the “leaky” $\binom{2}{1}$ –ROT, Protocol 2.17, is not secure because it leaks some information. Commonly in such a case one would use privacy amplification techniques to achieve security from this less secure protocol. Typically this involves applying a hash function with a seed that is picked by Alice and later announced to Bob, after he has measured the received qubits or messages.

In the isolated qubits model however, the use of such techniques is not possible since Bob is allowed to wait and measure the qubits at a later point, in this case after learning the seed of the hash function used for privacy amplification. A privacy amplification technique such as this would at best have no effect or even allow a dishonest user Bob to use that information to attack the protocol. In [Liu15], Liu presented a technique for privacy amplification in the isolated qubits model by fixing two r -wise independent hash functions at the beginning of the protocol, and applying them on the outputs of the “leaky” $\binom{2}{1}$ –ROT protocol.

3.1.1 Protocol String $\binom{2}{1}$ –ROT

We introduce a protocol for string $\binom{2}{1}$ –ROT based on the protocol proposed by Liu [Liu14b] and the privacy amplification technique that uses two fixed r -wise independent hash functions.

Protocol 3.1. A protocol for string $\binom{2}{1}$ -ROT between user Alice with no input and Bob with input $D \in \{0, 1\}$.

1. Alice chooses two r -wise independent hash functions F and G uniformly at random.
2. Alice with no input and Bob with input D use a “leaky” string $\binom{2}{1}$ -ROT (such as Protocol 2.17). Alice receives as output two messages $s, t \in \{0, 1\}^\ell$ and Bob, depending on his choice, receives s if $D = 0$ or t if $D = 1$.
3. Alice receives output $A_0, A_1 \in \{0, 1\}^{\ell'}$ such that:

$$A_0 = F(s) \tag{3.1}$$

$$A_1 = G(t) \tag{3.2}$$

4. Bob computes $F(s)$ or $G(t)$, depending on his input D and obtains A_D .

3.1.2 Security Of The Protocol

It is not difficult to see that if the “leaky” string $\binom{2}{1}$ -ROT is correct then Protocol 3.1 is correct. Furthermore since the protocol is non-interactive Alice learns nothing about Bob’s actions, as is reasoned in [Liu15].

The security for Alice of an $\binom{2}{1}$ -ROT, Definition 2.9, is equivalent to the following definition, that was used in [Liu15]:

Definition 3.2. We say that Protocol 3.1 is secure if the following holds: Let $k \geq 1$ be a security parameter. Suppose Alice receives as output two messages $A_0, A_1 \in \{0, 1\}$. Consider any dishonest LOCC user Bob, and let Z be the random variable representing the results of Bob’s measurements. Then there exists a random variable $D \in \{0, 1\}$ such that:

$$\|P_{A_{1-D}A_D D Z} - P_{U^{\ell'}} \times P_{A_D D Z}\|_1 \leq 2^{-\Omega(k)}, \tag{3.3}$$

where $U^{\ell'}$ denotes the uniform distribution on $\{0, 1\}^{\ell'}$.

Theorem 3.3 then states that we can reduce a secure string $\binom{2}{1}$ -ROT protocol (Protocol 3.1) to a “leaky” string $\binom{2}{1}$ -ROT protocol (Protocol 2.17). That is if there exists a protocol with output two strings $s, t \in \{0, 1\}^\ell$ and leaking any constant fraction of information of s and t , then we can construct a $\binom{2}{1}$ -ROT where Alice receives two strings $A_0, A_1 \in \{0, 1\}^{\ell'}$ and only allows an exponentially small amount of information about either A_0 or A_1 to leak, and is thus secure.

Theorem 3.3. For any constants $\theta \geq 1$, $\delta_0 > 0$, $\alpha > 0$, $\varepsilon_0 > 0$ and $0 < \kappa < \min\left\{\frac{\delta_0}{2}, \frac{\varepsilon_0}{2}, \frac{\alpha}{4}\right\}$ there exists a constant $k_0 \geq 1$ such that:

Suppose we have a “leaky” $\binom{2}{1}$ -ROT protocol in the isolated qubits model, such as Protocol 2.17, indexed by a security parameter $k \geq k_0$. More precisely, suppose that for all $k \geq k_0$,

1. Alice receives as output from Protocol 2.17 two messages $s, t \in \{0, 1\}^\ell$, where $\ell \geq k$ and uses m qubits, where $k \leq m \leq k^\theta$.

2. *Correctness:* For honest users, Alice receives s and t and Bob receives s if $D = 0$ or t if $D = 1$, using only LOCC operations.
3. *“Leaky” security:* Let $\delta_0 > 0$ be any constant, and set $\delta = 2^{-\delta_0 k}$. Honest user Alice receives outputs $s, t \in \{0, 1\}^\ell$. For any dishonest LOCC Bob, let Z be the random variable representing the result of his measurement. Let M be any separable measurement outcome M that is δ -non-negligible. Then:

$$H_\infty^\varepsilon(S, T | Z = M) \geq \alpha k, \quad (3.4)$$

where $\varepsilon \leq 2^{-\varepsilon_0 k}$.

Now assume Alice and Bob use Protocol 3.1, with r -wise independent hash functions $F, G : \{0, 1\}^\ell \mapsto \{0, 1\}^{\ell'}$, with

$$r = 4(\gamma + 1)k^{2\theta} \quad (3.5)$$

and

$$\ell' = \kappa k. \quad (3.6)$$

This choice of r is motivated by the union bound, see equation (3.52). Here γ is some universal constant. The choice of ℓ' is motivated by equations (3.99), (3.100), (3.101) and (3.102)

Then Protocol 3.1 is a secure $\binom{2}{1}$ -ROT protocol in the isolated qubits model, in the sense of Definition 3.2. More precisely, for all $k \geq k_0$, the following statements hold, except with probability $e^{-\Omega(k^{2\theta})}$ over the choice of F and G :

1. Alice receives as output from Protocol 3.1 two messages $A_0, A_1 \in \{0, 1\}^{\ell'}$ and uses m qubits, where $k \leq m \leq k^\theta$.
2. *Correctness:* For honest users Alice with no input and Bob with input D , Alice receives A_0 and A_1 and Bob receives A_D , using only LOCC operations.
3. *“Ideal” security:* For honest Alice with outputs (A_0, A_1) from Protocol 3.1, for any dishonest LOCC user Bob, let Z be the random variable representing the results of his measurements. Then there exists a random variable $D \in \{0, 1\}$, such that:

$$\begin{aligned} & \|P_{A_1-D A_D D Z} - P_U \times P_{A_D D Z}\|_1 \\ & \leq 2^{-(\delta_0 k - 2(\ell' + 1))} + 2^{-(\varepsilon_0 k - 2\ell' + 3)} + 2^{-(\frac{\alpha}{2} k - 2(\ell' + 1))} + 2^{-(\frac{\alpha}{2} k - 2(\ell' + 2 + \theta \ln k) - \ln(\gamma + 1))} \\ & \leq 2^{-\Omega(k)}, \end{aligned} \quad (3.7)$$

Before proving this theorem we present the definition of the ε' -obliviousness condition in order to introduce Theorem 3.5 that we use later to prove the security of Protocol 3.1.

Note that the ε' -obliviousness condition (for Random 1-2 OT $^\ell$) extended for strings [DFSS06, Definition 3.2] describes the security condition of Definition 3.2.

Definition 3.4. ε' -Obliviousness condition: For any LOCC adversary who observes the measurement outcome Z , there exists a binary random variable D such that

$$\|P_{A_1-D A_D D Z} - P_{U^\ell} \times P_{A_D D Z}\| \leq \varepsilon' \quad (3.8)$$

Moreover, we introduce [DFSS06, Theorem 4.5], that we will use to prove the security of Protocol 3.1.

Theorem 3.5. [DFSS06, Theorem 4.5] The ε' -obliviousness condition is satisfied for any LOCC adversary who observes the measurement outcome Z if and only if:

$$\forall \text{ non-degenerate linear function } \beta: \|P_{\beta(A_0, A_1) Z} - P_{U^\ell} \times P_Z\| \leq \frac{\varepsilon'}{2^{2\ell'+1}} \quad (3.9)$$

Theorem 3.5 states that it is enough to show that $\|P_{\beta(A_0, A_1) Z} - P_{U^\ell} \times P_Z\| \leq \frac{\varepsilon'}{2^{2\ell'+1}}$ for all non-degenerate linear functions β , in order to prove the security of the protocol.

3.2 Proof Of Theorem 3.3

In this section we prove Theorem 3.3 following the reasoning used in [Liu15]. We first show that with high probability over F and G the scheme is secure for any fixed separable measurement outcome M . Then we use the μ -net \widetilde{W} for the set of all separable measurement outcomes and show that Protocol 3.1 is secure at all points $\widetilde{M} \in \widetilde{W}$ with high probability. We then show that any separable measurement M can be approximated by a measurement outcome in the μ -net, $\widetilde{M} \in \widetilde{W}$. Then security at \widetilde{M} implies security at M for any separable measurement. Thus Protocol 3.1 is secure.

3.2.1 Security For Fixed Measurement M

First, we show that in the case when the adversary observes a fixed measurement outcome $Z = M$ the protocol is secure. Assuming that M is separable and δ -non-negligible, the “leaky” security guarantee implies $H_\infty^\varepsilon(S, T | Z = M) \geq \alpha k$ (equation (3.4)). The following lemma defines a smoothing event \mathcal{E} and the quantity $R^\beta(M)$ and states that $R^\beta(M)$ is small, with high probability over the choice of F and G .

Lemma 3.6. Fix any measurement outcome M such that $H_\infty^\varepsilon(S, T | Z = M) \geq \alpha k$. Then there exists an event \mathcal{E} , occurring with probability $P(\mathcal{E} | Z = M) \geq 1 - \varepsilon$, such that the following statement holds for all non-degenerate linear functions $\beta : \{0, 1\}^{\ell'} \times \{0, 1\}^{\ell'} \mapsto \{0, 1\}$:

We define:

$$R^\beta(M) = \mathbb{E}(1_{\mathcal{E}} \cdot (-1)^{\beta(A_0, A_1)} | Z = M), \quad (3.10)$$

which is a random variable depending on F , G , S and T , since $A_0 = F(S)$ and $A_1 = G(T)$. Then for all $\lambda > 0$ and for all non-degenerate linear functions β ,

$$P_{F, G, S, T}(|R^\beta(M)| \geq \lambda) \leq 8e^{1/(3r)} \sqrt{\pi r} \left(\frac{8 \cdot 2^{-\alpha k} r^2}{e^2 \lambda^2} \right)^{r/4}. \quad (3.11)$$

Proof. From $H_\infty^\varepsilon(S, T | Z = M) \geq \alpha k$, there exists a smoothing event \mathcal{E} , occurring with probability $P(\mathcal{E} | Z = M) \geq 1 - \varepsilon$, such that:

$$\forall s, t \in \{0, 1\}^\ell, P(\mathcal{E}, S = s, T = t | Z = M) \leq 2^{-\alpha k}. \quad (3.12)$$

Then the following holds:

$$\begin{aligned} \sum_{s, t \in \{0, 1\}^\ell} P(\mathcal{E}, S = s, T = t | Z = M)^2 \\ &= \sum_{s, t \in \{0, 1\}^\ell} P(\mathcal{E}, S = s, T = t | Z = M) \cdot P(\mathcal{E}, S = s, T = t | Z = M) \\ &\leq \sum_{s, t \in \{0, 1\}^\ell} 2^{-\alpha k} \cdot P(\mathcal{E}, S = s, T = t | Z = M) \\ &= 2^{-\alpha k} \cdot \sum_{s, t \in \{0, 1\}^\ell} P(\mathcal{E}, S = s, T = t | Z = M) \\ &\leq 2^{-\alpha k} \end{aligned} \quad (3.13)$$

We now bound the quantity $R^\beta(M)$ in a similar way as in [Liu15]. For a non-degenerate linear function β defined by non-zero strings u_0, u_1 , $\beta(A_0, A_1) = \langle u_0, F(s) \rangle + \langle u_1, G(t) \rangle$, where by definition $A_0 = F(s)$ and $A_1 = G(t)$. We then rewrite $R^\beta(M)$ as

$$R^\beta(M) = \sum_{s, t \in \{0, 1\}^\ell} (-1)^{\langle u_0, F(s) \rangle + \langle u_1, G(t) \rangle} P(\mathcal{E}, S = s, T = t | Z = M). \quad (3.14)$$

Firstly, we define a function $H : \{0, 1\} \times \{0, 1\}^\ell \rightarrow \{0, 1\}$:

$$H(i, s) = \begin{cases} \langle u_0, F(s) \rangle, & \text{if } i = 0 \\ \langle u_1, G(s) \rangle, & \text{if } i = 1, \end{cases} \quad (3.15)$$

for two non-zero $u_0, u_1 \in \{0, 1\}^\ell$.

Note that since F, G are r -wise independent hash functions and u_0, u_1 are non-zero strings then $\langle u_0, F(s) \rangle$ and $\langle u_1, G(s) \rangle$ are also r -wise independent hash functions.

By definition, F is a r -wise independent hash function if for all subsets $S \subset \{0, 1\}^\ell$ of size $|S| \leq r$, the random variables $\{F(x) | x \in S\}$ are independent and uniformly distributed in $\{0, 1\}^\ell$. Then the random variables $\{\langle u_0, F(x) \rangle | x \in S\}$ are also independent, where $\langle u_0, F(x) \rangle = \bigoplus_{i=1}^{\ell'} u_{0,i} \cdot \{F(x)\}_i$. Furthermore, from the fact that all non-degenerate linear functions are 2-balanced, Lemma 2.3, and from the definition of 2-balanced functions, Definition 2.2, we can see that since u_0 is non-zero the random variables $\{\langle u_0, F(x) \rangle | x \in S\}$ are uniformly distributed. (The same holds for $\{\langle u_1, G(x) \rangle | x \in S\}$).

Secondly, we define a matrix $A \in \mathbb{R}^{(2 \cdot 2^\ell) \times (2 \cdot 2^\ell)}$ with entries $A_{(i,s)(j,t)}$, for $i, j \in \{0, 1\}$ and $s, t \in \{0, 1\}^\ell$, that take the values:

$$A_{(i,s)(j,t)} = \begin{cases} \frac{1}{2}P(\mathcal{E}, S = s, T = t \mid Z = M) & \text{if } (i, j) = (0, 1) \\ \frac{1}{2}P(\mathcal{E}, S = t, T = s \mid Z = M) & \text{if } (i, j) = (1, 0) \\ 0 & \text{otherwise.} \end{cases} \quad (3.16)$$

Finally, using equation (3.15) and equation (3.16), $R^\beta(M)$ can be written in the following way,

$$R^\beta(M) = \mathbb{E}(1_{\mathcal{E}} \cdot (-1)^{\beta(A_0, A_1)} \mid Z = M) \quad (3.17)$$

$$= \sum_{s, t \in \{0, 1\}^\ell} P(\mathcal{E}, S = s, T = t \mid Z = M) (-1)^{\langle u_0, F(s) \rangle + \langle u_1, G(t) \rangle} \quad (3.18)$$

$$= \sum_{s, t \in \{0, 1\}^\ell} \left\{ \frac{1}{2}P(\mathcal{E}, S = s, T = t \mid Z = M) (-1)^{\langle u_0, F(s) \rangle + \langle u_1, G(t) \rangle} \right. \quad (3.19)$$

$$\left. + \frac{1}{2}P(\mathcal{E}, S = t, T = s \mid Z = M) (-1)^{\langle u_1, G(t) \rangle + \langle u_0, F(s) \rangle} \right\} \quad (3.20)$$

$$= \sum_{(i,s)(j,t)} A_{(i,s)(j,t)} ((-1)^{H(i,s)} (-1)^{H(j,t)} - \delta_{(i,s)(j,t)}) \quad (3.21)$$

Since $\langle u_0, F \rangle$ and $\langle u_1, G \rangle$ are r -wise independent random functions, we can set $t = r/2$ and use Proposition 2.5, using the following bounds on \tilde{A} :

$$\begin{aligned} \|\tilde{A}\|^2 &\leq \|\tilde{A}\|_F^2 = \sum_{(i,s)(j,t)} A_{(i,s)(j,t)}^2 \\ &= \frac{1}{2} \sum_{s, t} P(\mathcal{E}, S = s, T = t \mid Z = M)^2 \\ &\leq \frac{1}{2} \cdot 2^{-\alpha k}, \end{aligned} \quad (3.22)$$

where in the last line we used equation (3.13). Then by substituting into Proposition 2.5 we prove equation (3.11). We thus prove Lemma 3.6. \square

Next, we introduce Lemma 3.7 that implies that if $R^\beta(M)$ is small, we can use Theorem 3.5 to prove the security of the protocol when the adversary observes the measurement outcome M .

Lemma 3.7. *Fix any measurement outcome M . Suppose $|R^\beta(M)| \leq \xi$. Then:*

$$\|P_{\beta(A_0, A_1), \mathcal{E} \mid Z=M} - P_U\| \leq \xi + \varepsilon \quad (3.23)$$

Proof. Fix a measurement outcome M and suppose $|R^\beta(M)| \leq \xi$. From the definition of $R^\beta(M)$ we have that:

$$R^\beta(M) = \mathbb{E}(1_{\mathcal{E}} \cdot (-1)^{\beta(A_0, A_1)} \mid Z = M) \quad (3.24)$$

$$= P(\beta(A_0, A_1) = 0, \mathcal{E} \mid Z = M) - P(\beta(A_0, A_1) = 1, \mathcal{E} \mid Z = M) \quad (3.25)$$

From $R^\beta(M) \leq \xi$:

$$-\xi \leq P(\beta(A_0, A_1) = 0, \mathcal{E} \mid Z = M) - P(\beta(A_0, A_1) = 1, \mathcal{E} \mid Z = M) \leq \xi \quad (3.26)$$

From $P(\mathcal{E} \mid Z = M) \geq 1 - \varepsilon$ and basic probability theory:

$$1 - \varepsilon \leq P(\mathcal{E} \mid Z = M) = P(\beta(A_0, A_1) = 0, \mathcal{E} \mid Z = M) + P(\beta(A_0, A_1) = 1, \mathcal{E} \mid Z = M) \leq 1 \quad (3.27)$$

Combining equation (3.26) with equation (3.27) we get:

$$\left| P(\beta(A_0, A_1) = 0, \mathcal{E} \mid Z = M) - \frac{1}{2} \right| \leq \frac{\xi + \varepsilon}{2} \quad (3.28)$$

and

$$\left| P(\beta(A_0, A_1) = 1, \mathcal{E} \mid Z = M) - \frac{1}{2} \right| \leq \frac{\xi + \varepsilon}{2} \quad (3.29)$$

Then the ℓ_1 distance between $P_{\beta(A_0, A_1), \mathcal{E} \mid Z=M}$ and P_U is:

$$\begin{aligned} \|P_{\beta(A_0, A_1), \mathcal{E} \mid Z=M} - P_U\| &= \left| P(\beta(A_0, A_1) = 0, \mathcal{E} \mid Z = M) - \frac{1}{2} \right| \\ &\quad + \left| P(\beta(A_0, A_1) = 1, \mathcal{E} \mid Z = M) - \frac{1}{2} \right| \\ &\leq \xi + \varepsilon \end{aligned} \quad (3.30)$$

□

Thus we have proven that if $R^\beta(M)$ is small, Lemma 3.7 together with Theorem 3.5 imply that Protocol 3.1 is secure against a dishonest user Bob that observes the measurement outcome M .

3.2.2 Security For μ -net

In [Liu15], it is shown that there exists an μ -net \widetilde{W} for the set of all possible separable measurement outcomes W with respect to the operator norm $\|\cdot\|$. In this section, we show that the protocol is secure for all the measurement outcomes in the μ -net.

First, we introduce the following lemma as presented and proved in [Liu15].

Lemma 3.8. [Liu15, Lemma 3.5] *For any $0 < \mu \leq 1$, there exists a set $\widetilde{W} \subset W$, of cardinality $|\widetilde{W}| \leq \left(\frac{9m}{\mu}\right)^{4m}$, which is a μ -net for W with respect to the operator norm $\|\cdot\|$.*

We then use Lemma 3.8, and set

$$\mu = 2^{-(\alpha/2)k} \cdot \frac{\delta^2}{4^m}, \quad (3.31)$$

The value of μ is chosen so that it is small enough to approximate any measurement outcome, see equation (3.88) in the next section.

Together with the fact that $k \leq m \leq k^\theta$ and $\delta = 2^{-\delta_0 k}$ the cardinality of \widetilde{W} is bounded by:

$$|\widetilde{W}| \leq \left(9m \cdot 2^{\frac{\alpha}{2}k} \frac{4^m}{\delta^2}\right)^{4m} = \left(2^{\log(9m) + \frac{\alpha}{2}k + 2\delta_0 k + 2m}\right)^{4m} \quad (3.32)$$

$$= 2^{4m \log(9m) + 4(\alpha/2 + 2\delta_0)km + 8m^2} \leq 2^{4m \log(9m) + (2\alpha + 8\delta_0 + 8)m^2} \leq 2^{4k^\theta \log(9k^\theta) + (2\alpha + 8\delta_0 + 8)k^{2\theta}} \quad (3.33)$$

$$= 2^{4k^\theta \log 9 + 4k^\theta \theta \log k + (2\alpha + 8\delta_0 + 8)k^{2\theta}}. \quad (3.34)$$

For sufficiently large k it holds that $\log k \leq k \leq k^\theta \leq k^{2\theta}$. This also implies that $k^\theta \log k \leq k^{2\theta}$. Then for all sufficiently large k ,

$$|\widetilde{W}| \leq 2^{4k^\theta \log 9 + 4k^\theta \theta \log k + (2\alpha + 8\delta_0 + 8)k^{2\theta}} \leq 2^{(4 \log 9 + 4\theta + 2\alpha + 8\delta_0 + 8)k^{2\theta}} \quad (3.35)$$

$$\leq 2^{\gamma k^{2\theta}}, \quad (3.36)$$

where γ is a constant.

Next we use Lemma 3.6 and we set

$$\lambda = 2^{-(\alpha/2)k} \cdot 2r. \quad (3.37)$$

Then we have that

$$P_{F,G;S,T}(|R^\beta(M)| \geq \lambda) \leq 8e^{1/3r} \sqrt{\pi r} (e^2/2)^{-r/4}. \quad (3.38)$$

Finally, using the union bound we show that with high probability for all $\widetilde{M} \in \widetilde{W}$ and all non-degenerate linear functions β , $R^\beta(\widetilde{M})$ is small.

$$P_{F,G;S,T}(\exists \widetilde{M} \in \widetilde{W}, \text{ s.t. } \widetilde{M} \text{ is } \delta\text{-non-negligible, and } \exists \beta \text{ s.t. } |R^\beta(\widetilde{M})| \geq \lambda) \quad (3.39)$$

$$\leq |\widetilde{W}| \cdot \sum_{\beta} P_{F,G;S,T}(|R^\beta(\widetilde{M})| \geq \lambda) \quad (3.40)$$

$$\leq |\widetilde{W}| \cdot 2^{2\ell'} \cdot P_{F,G;S,T}(|R^\beta(\widetilde{M})| \geq \lambda) \quad (3.41)$$

$$\leq 2^{\gamma k^{2\theta}} \cdot 2^{2\ell'} \cdot \left(8e^{1/(3r)} \sqrt{\pi r} (e^2/2)^{-r/4} \right) \quad (3.42)$$

$$\stackrel{r=4(\gamma+1)k^{2\theta}}{=} 2^{\gamma k^{2\theta} + 3 + (\gamma+1)k^{2\theta} + 2\ell'} \cdot e^{\frac{1}{12(\gamma+1)k^{2\theta}} + \frac{1}{2} \ln 4\pi(\gamma+1)k^{2\theta} + 2(\gamma+1)k^{2\theta}} \quad (3.43)$$

$$\stackrel{\ell' \equiv \kappa k}{=} \exp \left\{ (3 + (2\gamma + 1)k^{2\theta} + 2\kappa k) \ln 2 \right. \quad (3.44)$$

$$\left. + \frac{1}{12(\gamma + 1)k^{2\theta}} + \frac{1}{2} \ln 4\pi(\gamma + 1) + \theta \ln k - 2(\gamma + 1)k^{2\theta} \right\} \quad (3.45)$$

Since $k^{2\theta} \ln 2 > 0$ and $e^{k^{2\theta} \ln 2} \geq 1$ we multiply equation (3.45) with $e^{k^{2\theta} \ln 2}$.

Furthermore, using the fact that

$$f(k) = 2\kappa k \ln 2 + \theta \ln k + \frac{1}{12(\gamma + 1)k^{2\theta}} + 3 \ln 2 + \frac{1}{2} \ln 4\pi(\gamma + 1) = o(k^2), \quad (3.46)$$

since

$$\lim_{k \rightarrow \infty} \frac{f(k)}{k^2} = \lim_{k \rightarrow \infty} \frac{2\kappa k \ln 2 \ln k + \frac{1}{12(\gamma+1)k^{2\theta}} + 3 \ln 2 + \frac{1}{2} \ln 4\pi(\gamma + 1)}{k^2} = 0, \quad (3.47)$$

equation (3.45) becomes:

$$\exp \left\{ (2\gamma + 1)k^{2\theta} \ln 2 - 2(\gamma + 1)k^{2\theta} + 2\kappa k \ln 2 + \theta \ln k \right. \quad (3.48)$$

$$\left. + \frac{1}{12(\gamma + 1)k^{2\theta}} + 3 \ln 2 + \frac{1}{2} \ln 4\pi(\gamma + 1) \right\} \quad (3.49)$$

$$\leq \exp \left\{ 2(\gamma + 1)(\ln 2 - 1)k^{2\theta} + o(k^2) \right\} \quad (3.50)$$

$$= \exp \left\{ - \left(2(\gamma + 1)(1 - \ln 2)k^{2\theta} - o(k^2) \right) \right\}. \quad (3.51)$$

Thus

$$P_{F,G;S,T}(\exists \widetilde{M} \in \widetilde{W}, \text{ s.t. } \widetilde{M} \text{ is } \delta\text{-non-negligible, and } \exists \beta \text{ s.t. } |R^\beta(\widetilde{M})| \geq \lambda) \leq e^{-\Omega(k^{2\theta})}. \quad (3.52)$$

Equation (3.52) implies that with high probability over F and G ,

$$\forall \widetilde{M} \in \widetilde{W}, (\widetilde{M} \text{ is } \delta\text{-non-negligible}) \Rightarrow |R^\beta(\widetilde{M})| \leq \lambda. \quad (3.53)$$

Thus Protocol 3.1 is secure in the case where the adversary observes any measurement outcome in the set \widetilde{W} .

3.2.3 Approximating Measurement Outcomes

We now show that any measurement outcome M can be approximated by another measurement outcome \widetilde{M} , just as in [Liu15].

First, we introduce a lemma proved and used in [Liu15] that shows that if M is 2δ -non-negligible then \widetilde{M} is δ -non-negligible.

Lemma 3.9. [Liu15, Lemma 3.6] *Suppose that $M, \widetilde{M} \in (\mathbb{C}^{2 \times 2})^{\otimes m}$, and $0 \preceq M \preceq I$, and $0 \preceq \widetilde{M} \preceq I$. Suppose that M is 2δ -non-negligible, where $0 < \delta \leq \frac{1}{2}$, and $\text{tr}(M) \geq 1$. Suppose that \widetilde{M} satisfies $\|M - \widetilde{M}\| \leq \mu$, where $\mu \leq \frac{2}{3}\delta \cdot 2^{-m}$. Then \widetilde{M} is δ -non-negligible.*

The next lemma shows that if the quantity $R^\beta(\widetilde{M})$ is defined in terms of an event $\widetilde{\mathcal{E}}$, we can define the quantity $R^\beta(M)$ by choosing \mathcal{E} such that $R^\beta(M) \approx R^\beta(\widetilde{M})$.

Lemma 3.10. *Suppose that $M, \widetilde{M} \in (\mathbb{C}^{2 \times 2})^{\otimes m}$, and $0 \preceq M \preceq I$, and $0 \preceq \widetilde{M} \preceq I$. Suppose that M is 2δ -non-negligible, where $0 < \delta \leq \frac{1}{2}$, and $\|M\| = 1$. Suppose that \widetilde{M} satisfies $\|M - \widetilde{M}\| \leq \mu$, where $\mu \leq \frac{1}{2}$, and \widetilde{M} is δ -non-negligible.*

Suppose there exists an event $\widetilde{\mathcal{E}}$, occurring with probability $P(\widetilde{\mathcal{E}} | \widetilde{Z} = \widetilde{M})$; and let $R^\beta(\widetilde{M})$ be defined in terms of $\widetilde{\mathcal{E}}$, as shown in equation (3.10).

Then there exists an event \mathcal{E} , occurring with probability $P(\mathcal{E} | Z = M) = P(\widetilde{\mathcal{E}} | \widetilde{Z} = \widetilde{M})$, such that if $R^\beta(M)$ is defined in terms of \mathcal{E} , then the following statement holds:

$$|R^\beta(M) - R^\beta(\widetilde{M})| \leq 2\mu \left(\frac{2^m}{\delta} \right)^2. \quad (3.54)$$

Proof. By assumption, there is an event $\widetilde{\mathcal{E}}$, defined by the probabilities $P(\widetilde{\mathcal{E}} | \widetilde{Z} = \widetilde{M}, S = s, T = t)$. Let ρ_{st} be the quantum state used to encode messages (s, t) , i.e., this is the state of the one-time memory, conditioned on $S = s$ and $T = t$.

We start by writing $R^\beta(\widetilde{M})$ in a more explicit form. First consider $R^\beta(\widetilde{M})$, and note that $A_0 = F(S)$, $A_1 = G(T)$ and s, t are chosen uniformly at random. We can write $R^\beta(\widetilde{M})$ in the form:

$$\begin{aligned} R^\beta(\widetilde{M}) &= \frac{1}{P(\widetilde{Z} = \widetilde{M})} \sum_{s, t \in \{0, 1\}^\ell} (-1)^{\beta(F(s), G(t))} P(\widetilde{\mathcal{E}}, S = s, T = t, \widetilde{Z} = \widetilde{M}) \\ &= \frac{1}{P(\widetilde{Z} = \widetilde{M})} \sum_{s, t \in \{0, 1\}^\ell} (-1)^{\beta(F(s), G(t))} P(\widetilde{\mathcal{E}}, | \widetilde{Z} = \widetilde{M}, S = s, T = t) \text{tr}(\widetilde{M} \rho_{st}) 4^{-\ell} \quad (3.55) \\ &= \frac{1}{P(\widetilde{Z} = \widetilde{M})} \text{tr}(\widetilde{M} \nu), \end{aligned}$$

where we define the matrix $\nu \in (\mathbb{C}^{2 \times 2})^{\otimes m}$ as follows:

$$\nu = 4^{-\ell} \sum_{s,t \in \{0,1\}^\ell} (-1)^{\beta(F(s), G(t))} P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \rho_{st}. \quad (3.56)$$

The trace norm of ν is $\|\nu\|_{\text{tr}} = \text{tr}(\sqrt{\nu \nu^\dagger})$. But note that

$$\nu^\dagger = \left(4^{-l} \sum_{s,t} (-1)^{\beta(F(s), G(t))} P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \rho_{st} \right)^\dagger \quad (3.57)$$

$$= 4^{-l} \sum_{s,t} (-1)^{\beta(F(s), G(t))} P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \rho_{st}^\dagger \quad (3.58)$$

Since density operators are self-adjoint $\rho_{st}^\dagger = \rho_{st}$. Then

$$\nu^\dagger = 4^{-l} \sum_{s,t} (-1)^{\beta(F(s), G(t))} P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \rho_{st} = \nu. \quad (3.59)$$

Then the trace norm is:

$$\|\nu\|_{\text{tr}} = \text{tr}(4^{-l} \sum_{s,t} (-1)^{\beta(F(s), G(t))} P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \rho_{st}) \quad (3.60)$$

$$= 4^{-l} \sum_{s,t} (-1)^{\beta(F(s), G(t))} P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \text{tr}(\rho_{st}) \quad (3.61)$$

Since ρ_{st} is a density operator $\text{tr}(\rho_{st}) = 1$ and because

$$P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \leq 1 \quad (3.62)$$

$$\Rightarrow (-1)^{\beta(F(s), G(t))} P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \leq 1 \quad (3.63)$$

$$\Rightarrow \sum_{s,t} (-1)^{\beta(F(s), G(t))} P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \leq 4^l \quad (3.64)$$

we get:

$$\|\nu\|_{\text{tr}} = 4^{-l} \sum_{s,t} (-1)^{\beta(F(s), G(t))} P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \leq 4^{-l} \cdot 4^l. \quad (3.65)$$

Thus $\|\nu\|_{\text{tr}} \leq 1$.

In addition, we can rewrite $P(\tilde{Z} = \tilde{M})$ in the following way:

$$\begin{aligned}
P(\tilde{Z} = \tilde{M}) &= \sum_{s,t \in \{0,1\}^\ell} P(\tilde{Z} = \tilde{M}, S = s, T = t) \\
&= \sum_{s,t \in \{0,1\}^\ell} \text{tr}(\tilde{M} \rho_{st}) 4^{-\ell} \\
&= \text{tr} \left(\tilde{M} \left(4^{-\ell} \sum_{s,t \in \{0,1\}^\ell} \rho_{st} \right) \right) \\
&= \text{tr}(\tilde{M} \xi),
\end{aligned} \tag{3.66}$$

where we define the matrix $\xi \in (\mathbb{C}^{2 \times 2})^{\otimes m}$ as follows:

$$\xi = 4^{-\ell} \sum_{s,t \in \{0,1\}^\ell} \rho_{st}. \tag{3.67}$$

Also, note that $\|\xi\|_{\text{tr}} \leq 1$.

Taking into account equation (3.55) and equation (3.66) we can rewrite $R^\beta(\tilde{M})$ as

$$R^\beta(\tilde{M}) = \frac{\text{tr}(\tilde{M} \nu)}{\text{tr}(\tilde{M} \xi)}, \tag{3.68}$$

where $\nu, \xi \in (\mathbb{C}^{2 \times 2})^{\otimes m}$ satisfy $\|\nu\|_{\text{tr}} \leq 1$ and $\|\xi\|_{\text{tr}} \leq 1$.

We now consider the measurement outcome M . We construct an event \mathcal{E} in order to define the quantity $R^\beta(M)$. The event \mathcal{E} conditioned on $Z = M$ behaves similarly to $\tilde{\mathcal{E}}$ conditioned on $\tilde{Z} = \tilde{M}$.

We now construct the event \mathcal{E} . For a fixed measurement outcome M and for all $s, t \in \{0, 1\}^\ell$ we define:

$$P(\mathcal{E} | Z = M, S = s, T = t) = P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M}, S = s, T = t) \tag{3.69}$$

Note that this implies $P(\mathcal{E} | Z = M) = P(\tilde{\mathcal{E}} | \tilde{Z} = \tilde{M})$. Using this we can rewrite the quantity $R^\beta(M)$ in a similar way as $R^\beta(\tilde{M})$:

$$R^\beta(M) = \frac{\text{tr}(M \nu)}{\text{tr}(M \xi)}, \tag{3.70}$$

where ν and ξ are the *same* matrices used to express $R^\beta(\widetilde{M})$ in equation (3.68). In addition, we can lower-bound $\text{tr}(M\xi)$ and $\text{tr}(\widetilde{M}\xi)$ as follows:

$$\text{tr}(M\xi) \geq 2\delta \cdot 2^{-m} \text{tr}(M) \geq 2\delta \cdot 2^{-m} \|M\| \quad (3.71)$$

$$\geq 2\delta \cdot 2^{-m}, \quad (3.72)$$

$$\text{tr}(\widetilde{M}\xi) \geq \delta \cdot 2^{-m} \text{tr}(\widetilde{M}) \quad (3.73)$$

$$\geq \delta \cdot 2^{-m} \|\widetilde{M}\| \quad (3.74)$$

$$\geq \delta \cdot 2^{-m} (1 - \mu) \geq \delta \cdot 2^{-m} \cdot \frac{1}{2}. \quad (3.75)$$

Where we used that M is 2δ -non-negligible, \widetilde{M} is δ -non-negligible and the inequalities (3.85) and (3.78).

Note that we use equation (3.86) and $\|M\| = 1$ to get:

$$\|M\| = \|M - \widetilde{M} + \widetilde{M}\| \leq \|M - \widetilde{M}\| + \|\widetilde{M}\| \quad (3.76)$$

$$\implies 1 \leq \mu + \|\widetilde{M}\| \quad (3.77)$$

$$\implies \|\widetilde{M}\| \geq 1 - \mu \quad (3.78)$$

We also used the fact that $\mu \leq \frac{2}{3} \cdot \delta \cdot 2^{-m}$, $\delta \leq \frac{1}{2}$ and $m \geq k \geq k_0 \geq 1$ (as defined in [Liu15]) to lower bound $1 - \mu$ as follows:

$$1 - \mu \geq 1 - \frac{2}{3} \cdot \delta \cdot 2^{-m} \geq 1 - \frac{1}{3} \cdot 2^{-m} \geq 1 - \frac{1}{6} \geq \frac{1}{2} \quad (3.79)$$

Now we can write $R^\beta(M) - R^\beta(\widetilde{M})$ as follows:

$$R^\beta(M) - R^\beta(\widetilde{M}) = \frac{\text{tr}(M\nu)}{\text{tr}(M\xi)} - \frac{\text{tr}(\widetilde{M}\nu)}{\text{tr}(\widetilde{M}\xi)} \quad (3.80)$$

$$= \frac{\text{tr}(M\nu)}{\text{tr}(M\xi)} - \frac{\text{tr}(\widetilde{M}\nu)}{\text{tr}(M\xi)} + \frac{\text{tr}(\widetilde{M}\nu)}{\text{tr}(M\xi)} - \frac{\text{tr}(\widetilde{M}\nu)}{\text{tr}(\widetilde{M}\xi)} \quad (3.81)$$

$$= \frac{\text{tr}(M\nu) - \text{tr}(\widetilde{M}\nu)}{\text{tr}(M\xi)} + \frac{\text{tr}(\widetilde{M}\nu) \text{tr}(\widetilde{M}\xi)}{\text{tr}(M\xi) \text{tr}(\widetilde{M}\xi)} - \frac{\text{tr}(\widetilde{M}\nu) \text{tr}(M\xi)}{\text{tr}(M\xi) \text{tr}(\widetilde{M}\xi)} \quad (3.82)$$

$$= \frac{\text{tr}((M - \widetilde{M})\nu)}{\text{tr}(M\xi)} + \text{tr}(\widetilde{M}\nu) \frac{\text{tr}((\widetilde{M} - M)\xi)}{\text{tr}(M\xi) \text{tr}(\widetilde{M}\xi)}. \quad (3.83)$$

We can then upper-bound this quantity:

$$\begin{aligned} |R^\beta(M) - R^\beta(\widetilde{M})| &\leq \frac{\mu}{2\delta \cdot 2^{-m}} + (1 + \mu) \frac{\mu}{2\delta \cdot 2^{-m} \cdot \delta \cdot 2^{-m} \cdot \frac{1}{2}} \\ &= \frac{\mu}{2\delta \cdot 2^{-m}} \left(1 + \frac{(1 + \mu)}{\delta \cdot 2^{-m} \cdot \frac{1}{2}} \right) \\ &\leq 2\mu \left(\frac{2^m}{\delta} \right)^2. \end{aligned} \quad (3.84)$$

This completes the proof of Lemma 3.10. \square

From Lemma 3.10 we can show that Protocol 3.1 is secure, when the adversary observes any separable measurement outcome $M \in W$ that is 2δ -non-negligible.

Note that $\|M\| = 1$ (that is assumed without loss of generality [Liu15]) implies $\text{tr}(M) \geq 1$:

$$\text{tr}(M) \geq 1 \quad (3.85)$$

Let $\widetilde{M} \in \widetilde{W}$ be the nearest point in the μ -net \widetilde{W} . Then we have:

$$\|M - \widetilde{M}\| \leq \mu, \quad (3.86)$$

where $\mu = 2^{-(\alpha/2)k} \frac{\delta^2}{4^m}$.

Then from Lemma 3.9, \widetilde{M} is δ -non-negligible. Then from equation (3.53) we get that $|R^\beta(\widetilde{M})| \leq \lambda$, where $\lambda = 2^{-(\alpha/2)k} \cdot 2r$:

$$-2^{-\frac{\alpha}{2}k} \cdot 2r \leq R^\beta(\widetilde{M}) \leq 2^{-\frac{\alpha}{2}k} \cdot 2r. \quad (3.87)$$

Using Lemma 3.10 and substituting μ we get that:

$$|R^\beta(M) - R^\beta(\widetilde{M})| \leq 2\mu \left(\frac{2^m}{\delta} \right)^2 = 2 \cdot 2^{-(\alpha/2)k} \quad (3.88)$$

$$\implies -2 \cdot 2^{-(\alpha/2)k} \leq R^\beta(M) - R^\beta(\widetilde{M}) \leq 2 \cdot 2^{-(\alpha/2)k}. \quad (3.89)$$

By adding equations (3.87) and (3.89) we get:

$$-2^{-(\alpha/2)k} \cdot 2(r+1) \leq R^\beta(M) \leq 2^{-(\alpha/2)k} \cdot 2(r+1) \quad (3.90)$$

$$\implies |R^\beta(M)| \leq 2^{-\frac{\alpha}{2}k} \cdot 2(r+1) \quad (3.91)$$

Then from Lemma 3.7 we see that Protocol 3.1 is secure for all 2δ -non-negligible measurement outcomes $M \in W$ that a dishonest user Bob may observe:

$$\|P_{\beta(A_0, A_1)\mathcal{E}|Z=M} - P_U\| \leq 2^{-\frac{\alpha}{2}k} \cdot 2(r+1) + \varepsilon = 2^{-\frac{\alpha}{2}k} \cdot 2(r+1) + 2^{-\varepsilon_0 k} \leq 2^{-\Omega(k)}. \quad (3.92)$$

Consider any LOCC adversary, and let Z be the random variable representing the measurement outcome. We can then write:

$$\begin{aligned}
& \|P_{\beta(A_0, A_1)Z} - P_U \times P_Z\| \\
& \leq \sum_M P(Z = M) \|P_{\beta(A_0, A_1)|Z=M} - P_U\| \\
& \leq 2\delta + \sum_{M: M \text{ is } 2\delta\text{-non-negligible}} P(Z = M) \|P_{\beta(A_0, A_1)|Z=M} - P_U\|,
\end{aligned} \tag{3.93}$$

since $\sum_{M: M \text{ is } 2\delta\text{-negligible}} P(Z = M) \leq 2\delta$.

Taking into account the bound shown in equation (3.92) and the fact that $P(\neg \mathcal{E} | Z = M) \leq \varepsilon$, equation (3.93) becomes

$$\begin{aligned}
& \|P_{\beta(A_0, A_1)Z} - P_U \times P_Z\| \\
& \leq 2\delta + 2\varepsilon + \sum_{M: M \text{ is } 2\delta\text{-non-negligible}} P(Z = M) (\|P_{\beta(A_0, A_1), \mathcal{E}|Z=M} - P_U\|) \\
& \leq 2\delta + 2\varepsilon + 2^{-\frac{\alpha}{2}k} \cdot 2(r+1) + \varepsilon \\
& \leq 2 \cdot 2^{-\delta_0 k} + 3 \cdot 2^{-\varepsilon_0 k} + 2^{-\frac{\alpha}{2}k} \cdot 2(r+1).
\end{aligned} \tag{3.94}$$

Note that in the last step we use the definitions of $\delta = 2^{-\delta_0 k}$ and $\varepsilon = 2^{-\varepsilon_0 k}$.

Then Theorem 3.5 with $\ell' = \kappa k$, where $0 < \kappa < \min\left\{\frac{\delta_0}{2}, \frac{\varepsilon_0}{2}, \frac{\alpha}{4}\right\}$ and

$$\|P_{\beta(A_0, A_1)Z} - P_U \times P_Z\| \leq 2 \cdot 2^{-\delta_0 k} + 3 \cdot 2^{-\varepsilon_0 k} + 2^{-\frac{\alpha}{2}k} \cdot 2(r+1) = \frac{\varepsilon'}{2^{2\ell'+1}}, \tag{3.95}$$

implies that

$$\begin{aligned}
& \|P_{A_{1-D} A_D D Z} - P_{U^\ell} \times P_{A_D D Z}\| \leq \varepsilon' \\
& \leq 2^{2\ell'+1} \cdot \left(2 \cdot 2^{-\delta_0 k} + 3 \cdot 2^{-\varepsilon_0 k} + 2^{-\frac{\alpha}{2}k} \cdot 2(r+1)\right) \\
& \leq 2^{2\ell'+1} \cdot \left(2 \cdot 2^{-\delta_0 k} + 4 \cdot 2^{-\varepsilon_0 k} + 2^{-\frac{\alpha}{2}k} \cdot 2(r+1)\right) \\
& \leq 2^{-\delta_0 k + 2\ell' + 2} + 2^{-\varepsilon_0 k + 2\ell' + 3} + 2^{-\frac{\alpha}{2}k + 2\ell' + 2} + 2^{-\frac{\alpha}{2}k + 2\ell' + 2 + \ln r} \\
& \leq 2^{-(\delta_0 k - 2(\ell' + 1))} + 2^{-(\varepsilon_0 k - 2\ell' + 3)} + 2^{-(\frac{\alpha}{2}k - 2(\ell' + 1))} \\
& \quad + 2^{-(\frac{\alpha}{2}k - 2(\ell' + 2 + \theta \ln k) - \ln(\gamma + 1))}
\end{aligned} \tag{3.96}$$

Next we examine the term $2^{-(\delta_0 k - 2(\ell' + 1))}$, since $\ell' < \frac{\delta_0}{2}k$ then:

$$\exists c > 0 \exists k'_0 : \forall k > k'_0 \text{ the following holds: } \delta_0 k - 2(\ell' + 1) \geq ck \tag{3.97}$$

$$\implies \delta_0 k - 2(\ell' + 1) \in \Omega(k) \tag{3.98}$$

then we have that for sufficiently large k :

$$2^{-(\delta_0 k - 2(\ell' + 1))} \leq 2^{-\Omega(k)} \quad (3.99)$$

In a similar way we get that since $\ell' < \frac{\varepsilon_0}{2}k$ then for sufficiently large k :

$$2^{-(\varepsilon_0 k - 2\ell' + 3)} \leq 2^{-\Omega(k)} \quad (3.100)$$

Finally since $\ell' < \frac{\alpha}{4}k$ then for sufficiently large k

$$2^{-(\frac{\alpha}{2}k - 2(\ell' + 1))} \leq 2^{-\Omega(k)} \quad (3.101)$$

and

$$2^{-(\frac{\alpha}{2}k - 2(\ell' + 2 + \theta \ln k) - \ln(\gamma + 1))} = 2^{-(\frac{\alpha}{2}k - 2\ell' - o(k))} \leq 2^{-\Omega(k)}, \quad (3.102)$$

which holds since

$$f(k) = 2\theta \ln k + 4 + \ln(\gamma + 1) \in o(k). \quad (3.103)$$

Thus from equations (3.99), (3.100), (3.101) and (3.102), for sufficiently large k

$$\|P_{A_1 - D} A_D D Z - P_{U^\ell} \times P_{A_D D Z}\| \leq 2^{-\Omega(k)}, \quad (3.104)$$

which completes the proof of Theorem 3.3 □

Chapter 4

Flavours Of Oblivious Transfer

In the previous chapter, we showed that a secure string $\binom{2}{1}$ -ROT protocol can be constructed in the isolated qubits model. In this chapter we use the $\binom{2}{1}$ -ROT functionality to construct protocols that implement more complex oblivious transfer functionalities.

First we present a protocol that implements the $\binom{2}{1}$ -OT functionality using an instance of the $\binom{2}{1}$ -ROT functionality. As we have already discussed in Chapter 1, an $\binom{2}{1}$ -OT protocol is sufficient to implement any two-party computation securely, which makes it a fundamental problem in cryptography.

Secondly, we present a reduction from $\binom{k}{1}$ -OT and $\binom{k}{1}$ -ROT to a series of k $\binom{2}{1}$ -OTs, that was first introduced in [BCR86].

Finally, we construct a protocol that implements the weaker $\binom{k}{1}$ - $\widetilde{\text{ROT}}$ functionality using only $\log k$ $\binom{2}{1}$ -ROT functionalities.

These results are more general as these protocols are not restricted to the isolated qubits model as they rely on the existence and composability of a secure $\binom{2}{1}$ -ROT protocol in a cryptographic model.

4.1 $\binom{2}{1}$ -OT from $\binom{2}{1}$ -ROT

In this section, we introduce a protocol that implements the $\binom{2}{1}$ -OT functionality making use of a $\binom{2}{1}$ -ROT functionality. A sketch of Protocol 4.1 can be seen in Figure 4.1

Protocol 4.1. A $\binom{2}{1}$ -OT protocol between user Alice with inputs $A_0, A_1 \in \{0, 1\}^\ell$ and user Bob with input $D \in \{0, 1\}$.

1. Alice and Bob use a $\binom{2}{1}$ -ROT functionality with no input and input D respectively.
2. Alice receives outputs $S_0, S_1 \in \{0, 1\}^\ell$ and Bob receives $S_D \in \{0, 1\}^\ell$.
3. Alice then sends two messages Y_0, Y_1 such that:

$$Y_0 = S_0 \oplus A_0 \tag{4.1}$$

$$Y_1 = S_1 \oplus A_1 \tag{4.2}$$

4. Bob then receives output:

$$X_D = Y_D \oplus S_D \quad (4.3)$$

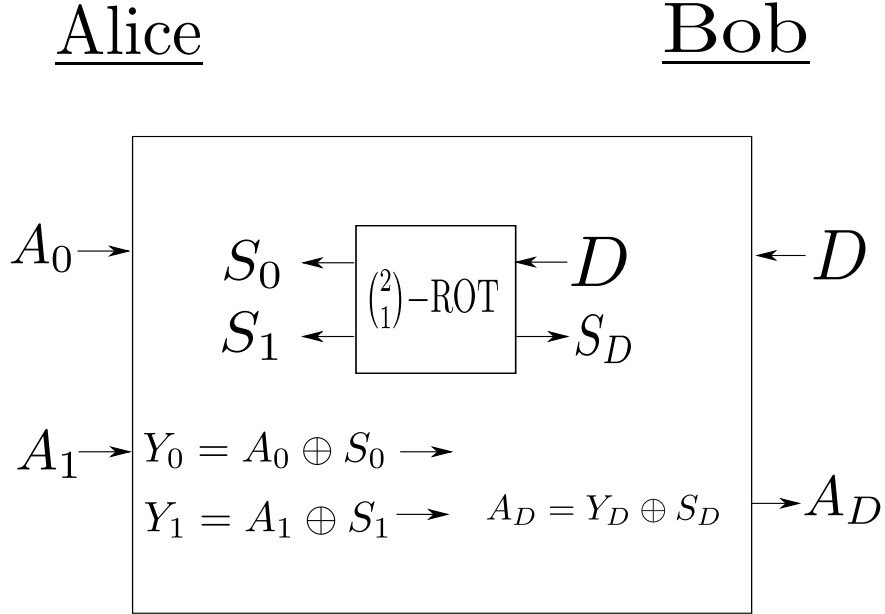


FIGURE 4.1: Sketch of the $\binom{2}{1}$ -OT Protocol 4.1 using a $\binom{2}{1}$ -ROT functionality.

We introduce the theorem that states that if the $\binom{2}{1}$ -ROT functionality is implemented securely, then so is the $\binom{2}{1}$ -OT functionality.

Theorem 4.2. *If the $\binom{2}{1}$ -ROT functionality used in Protocol 4.1 fulfills the ε -security Definition 2.9, then the $\binom{2}{1}$ -OT Protocol 4.1 is ε -secure according to Definition 2.7.*

4.1.1 Proof of Theorem 4.2

In order to prove Theorem 4.2 we need to show that all the conditions of Definition 2.7 are fulfilled.

4.1.1.1 Correctness

Proof. If both Alice and Bob are honest, they follow Protocol 4.1.

Then if the $\binom{2}{1}$ -ROT functionality is implemented correctly Alice will receive outputs S_0, S_1 and Bob will receive S_D except with probability ε .

After Alice sends Y_0, Y_1 , where $Y_i = A_i \oplus S_i$, Bob outputs $Y_D \oplus S_D = A_D$, implying correctness except with probability ε .

□

4.1.1.2 Security for Alice

Proof. For an honest user Alice, security of the $\binom{2}{1}$ -ROT functionality implies that there exists a random variable D' such that

$$P_{S_1-D'G'S_{D'}D'} \approx_\varepsilon P_U \cdot P_{G'S_{D'}D'}, \quad (4.4)$$

where S_0, S_1 are the outputs of honest Alice and G' is the output of a dishonest user Bob.

Define random variable $D'' = D'$, then since an honest user Alice does not use her inputs A_0, A_1 in the $\binom{2}{1}$ -ROT it is clear that

$$P_{G'D''S_0S_1A_0A_1} = P_{G'D''S_0S_1} \cdot P_{A_0A_1}, \quad (4.5)$$

which implies that

$$P_{D''A_0A_1} = P_{D''} \cdot P_{A_0A_1}. \quad (4.6)$$

Furthermore equation (4.5) implies that

$$P_{G'D''S_{D''}A_0A_1} = P_{G'S_{D''}|D''} \cdot P_{D''} \cdot P_{A_0A_1}, \quad (4.7)$$

and from equation (4.6) we have that

$$P_{G'D''S_{D''}A_0A_1} = P_{G'S_{D''}|D''} \cdot P_{A_0A_1D''}, \quad (4.8)$$

and

$$P_{G'D''S_{D''}A_0A_1} = P_{G'S_{D''}|D''A_{D''}} \cdot P_{A_{D''}A_1-D''D''}. \quad (4.9)$$

Bob's input G'' depends on G', Y_0, Y_1 , where $Y_0 = S_0 \oplus A_0$ and $Y_1 = S_1 \oplus A_1$.

Then from equation (4.4) and (4.5) we get

$$P_{S_{1-D''}G'D''S_{D''}A_{D''}} \approx_\varepsilon P_U \cdot P_{G'S_{D''}D''} \cdot P_{A_{D''}}, \quad (4.10)$$

which implies that

$$P_{S_{1-D''}|G'D''S_{D''}A_{D''}} \approx_\varepsilon P_U. \quad (4.11)$$

Then $Y_{1-D''}$ is independent of $A_{1-D''}$ given $G', D'', S_{D''}, A_{D''}$ and $Y_{D''} = A_{D''} \oplus S_{D''}$.

Therefore

$$P_{Y_0Y_1G'D''S_{D''}A_{D''}A_{1-D''}} \approx_\varepsilon P_{Y_0Y_1|G'D''S_{D''}A_{D''}} \cdot P_{G'D''S_{D''}A_{D''}} \cdot P_{A_{1-D''}} \quad (4.12)$$

and taking into account equation (4.9)

$$P_{Y_0Y_1G'D''S_{D''}A_{D''}A_{1-D''}} \approx_\varepsilon P_{Y_0Y_1|G'D''S_{D''}A_{D''}} \cdot P_{G'S_{D''}|D''A_{D''}} \cdot P_{D''A_{D''}A_{1-D''}} \quad (4.13)$$

$$\Rightarrow P_{G''D''A_{D''}A_{1-D''}} \approx_\varepsilon P_{G''|D''A_{D''}} \cdot P_{D''A_{D''}A_{1-D''}} \quad (4.14)$$

Thus, equations (4.6) and (4.14) imply that Protocol 4.1 is secure for Alice. \square

4.1.1.3 Security for Bob

Proof. If the $\binom{2}{1}$ -ROT functionality is secure for honest user Bob with input D , there exist random variables S'_0, S'_1 such that

$$P[G = S'_D] \geq 1 - \varepsilon \quad (4.15)$$

and

$$P_{S'_0S'_1D} \approx_\varepsilon P_{S'_0S'_1}P_D, \quad (4.16)$$

where D and G are Bob's input and output used in $F_{\binom{2}{1}\text{-ROT}}$.

We can then define random variables $A'_0 = Y_0 \oplus S'_0$ and $A'_1 = Y_1 \oplus S'_1$, where Y_0 and Y_1 are the messages sent by Alice to Bob after the $\binom{2}{1}$ -ROT.

Then from equation (4.16) and since Alice receives no further information from Bob after the $\binom{2}{1}$ -ROT has been used it is clear that

$$P_{A'_0 A'_1 D} \approx_\varepsilon P_{A'_0 A'_1} P_D. \quad (4.17)$$

Finally since Bob is honest, his output G' will be $G' = G \oplus Y_D$, which implies that

$$P[G = A'_D] \geq 1 - \varepsilon. \quad (4.18)$$

Thus Protocol 4.1 is secure for Bob. □

This completes the proof of Theorem 4.2.

4.2 $\binom{k}{1}$ -OT And $\binom{k}{1}$ -ROT From $\binom{2}{1}$ -OT

The following $\binom{k}{1}$ -OT protocol makes use of k $\binom{2}{1}$ -OT functionalities and was first presented in [BCR86].

Protocol 4.3. A $\binom{k}{1}$ -OT protocol between user Alice with inputs $X_1, \dots, X_k \in \{0, 1\}^\ell$ and user Bob with input $D \in \{1, \dots, k\}$.

1. Alice chooses strings $B_1, \dots, B_k \in \{0, 1\}^\ell$ uniformly at random.
2. Alice inputs $A_{1,0} = B_1$ and $A_{1,1} = X_1$ in the first $\binom{2}{1}$ -OT. Bob inputs his choice $D_1 = \delta_{1,D}$ and receives string A_{1,D_1} .
3. For $i = 2, \dots, k$:
 - (a) Alice inputs strings $A_{i,0} = B_i \oplus B_{i-1}$ and $A_{i,1} = X_i \oplus B_{i-1}$ in the i^{th} $\binom{2}{1}$ -OT.
 - (b) Bob inputs his i^{th} choice $D_i = \delta_{i,D}$ and receives the string A_{i,D_i} .
4. Bob receives output:

$$X_D = A_{D,1} \oplus \left(\bigoplus_{j=1}^{D-1} A_{j,0} \right) \quad (4.19)$$

It is easy to see that a $\binom{k}{1}$ -ROT protocol can be constructed if Alice chooses her input messages X_1, \dots, X_k uniformly at random. A sketch of the security proof for this protocol can be found in [BCR86]. We present this protocol and its possible extension to a $\binom{k}{1}$ -ROT protocol to argue that indeed such a protocol can be constructed from a secure $\binom{2}{1}$ -OT. However, it requires k (or $k-1$)¹ $\binom{2}{1}$ -OT functionalities. In the next section we present a protocol that fulfills a weaker security definition but requires only $\log k$ $\binom{2}{1}$ -ROTs. We will later use that protocol in Chapter 5 to achieve secure password-based identification.

¹This protocol can be implemented using $k-1$ $\binom{2}{1}$ -OTs if in the last $\binom{2}{1}$ -OT Alice inputs $A_{k,0} = B_{k-1} \oplus X_{k-1}$ and $A_{k,1} = B_{k-1} \oplus X_k$.

4.3 $\binom{k}{1} - \widetilde{\text{ROT}}$ from $\binom{2}{1} - \text{ROT}$

4.3.1 Protocol And Security Definition

In this section, we introduce a protocol that implements the $\binom{k}{1} - \widetilde{\text{ROT}}$ functionality. While the following $\binom{k}{1} - \widetilde{\text{ROT}}$ protocol fulfills a weaker security definition, it is more efficient than Protocol 4.3 or its extension to a $\binom{k}{1} - \text{ROT}$ as it makes use of only $\log k$ $\binom{2}{1} - \text{ROT}$ s instead of k $\binom{2}{1} - \text{OT}$ s.

Alice with no input, receives $\log k$ pairs of strings $(A_{i,0}, A_{i,1})$ from the i^{th} $\binom{2}{1} - \text{ROT}$, for $i \in \{1, \dots, \log k\}$. Her output messages S_1, \dots, S_k will later be composed of the possible additions of these strings, for example $S_1 = \bigoplus_{i=1}^{\log k} A_{i,0}$.

Bob with input $D \in \{1, \dots, k\}$, that can be seen as a string $\{D_1|D_2|\dots|D_{\log k}\}$, in turn inputs the i^{th} bit of his choice D_i to the i^{th} $\binom{2}{1} - \text{ROT}$ functionality and obtains output A_{i,D_i} . He finally adds the outputs he received to obtain his output of the $\binom{k}{1} - \widetilde{\text{ROT}}$ functionality $S_D = \bigoplus_{i=1}^{\log k} A_{i,D_i}$. A sketch of the protocol can be seen in Figure 4.2.

Protocol 4.4. *Sender-randomised $\binom{k}{1} - \widetilde{\text{ROT}}$ protocol between user Alice with no input and user Bob with input $D = \{D_1|D_2|\dots|D_{\log k}\} \in \{1, \dots, k\}$.*

1. For $i = 1, \dots, \log k$:

- (a) Alice with no input receives strings $A_{i,0}, A_{i,1} \in \{0, 1\}^\ell$ as outputs of the i^{th} $\binom{2}{1} - \text{ROT}$,
- (b) Bob inputs his i^{th} choice D_i and receives the string A_{i,D_i} .

2. Alice receives outputs:

$$\begin{aligned} S_1 &= A_{1,0} \oplus A_{2,0} \oplus \dots \oplus A_{\log k,0} \\ S_2 &= A_{1,1} \oplus A_{2,0} \oplus \dots \oplus A_{\log k,0} \\ &\vdots \\ S_k &= A_{1,1} \oplus A_{2,1} \oplus \dots \oplus A_{\log k,1} \end{aligned} \tag{4.20}$$

and Bob receives output:

$$S_D = \bigoplus_{i=1}^{\log k} A_{i,D_i} \tag{4.21}$$

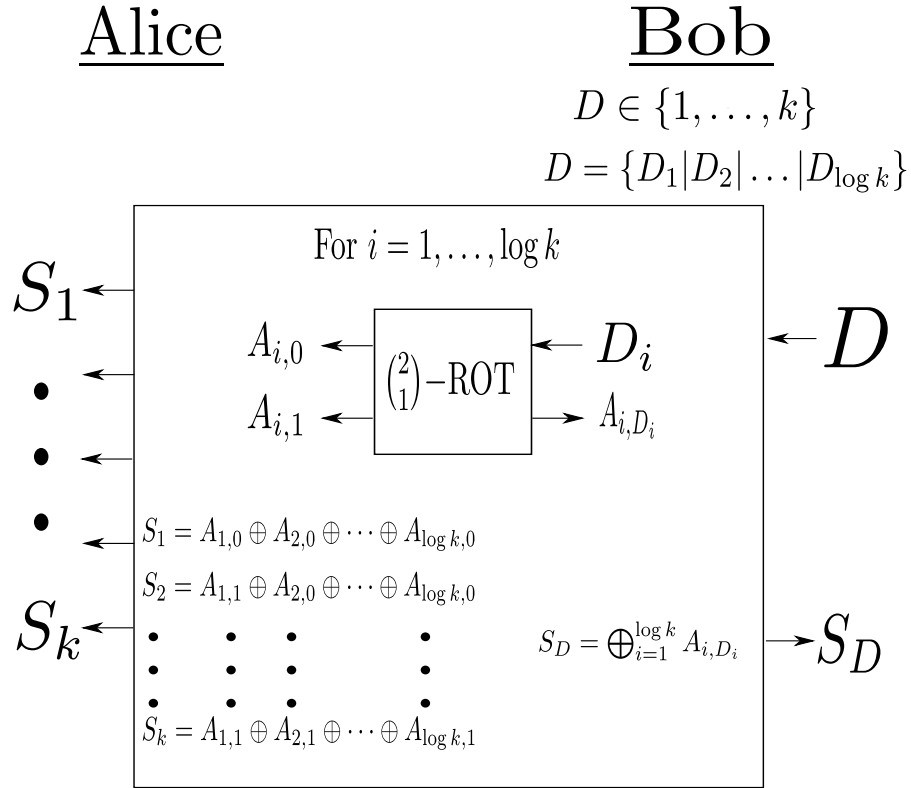


FIGURE 4.2: Sketch of the $\begin{pmatrix} k \\ 1 \end{pmatrix} - \widetilde{\text{ROT}}$ Protocol 4.4 using $\log k$ $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ -OT functionalities.

We now introduce the theorem that states that if the $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ -ROT functionalities used in the above protocol are secure, in the sense of Definition 2.7, then the protocol implements the $\begin{pmatrix} k \\ 1 \end{pmatrix} - \widetilde{\text{ROT}}$ functionality securely, according to the Definition 2.13.

Theorem 4.5. *If the $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ -ROT functionalities used in Protocol 4.4 are ε -secure, according to Definition 2.9, then Protocol 4.4 is ε' -secure according to Definition 2.14, where $\varepsilon' \leq \varepsilon \log k$.*

4.3.2 Proof Of Theorem 4.4

The following proof consists of three parts as we have to show that all three requirements of Definition 2.13 hold.

4.3.2.1 Correctness

First we show that the correctness requirement of Definition 2.14 holds if the correctness requirement of Definition 2.9 holds.

Proof. We show that for two honest users who follow Protocol 4.4, the protocol is correct if the $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ -ROT functionality is implemented correctly.

An honest user Alice receives outputs $(A_{i,0}, A_{i,1})$ from the i^{th} $\binom{2}{1}$ -ROT used in the protocol, for $i = 1, \dots, \log k$. She receives outputs $S_1 \dots S_k$ by modulo 2 addition of these inputs, for example $S_1 = \bigoplus_{i=1}^{\log k} A_{i,0}$.

Then Bob with input $D = \{D_1 | \dots | D_{\log k}\}$, uses D_i as input to the i^{th} $\binom{2}{1}$ -ROT. If the $\binom{2}{1}$ -ROTs are correct he receives A_{i,D_i} except with probability ε for all $i = 1, \dots, \log k$.

He then correctly computes $X_D = \bigoplus_{i=1}^{\log k} A_{i,D_i}$ except with probability $\varepsilon' \leq \varepsilon \cdot \log k$.

Thus Protocol 4.4 is correct. \square

4.3.2.2 Security For Alice

Secondly we show that if the $\binom{2}{1}$ -ROT are secure for Alice in the sense of Definition 2.9 then the security for Alice condition of Definition 2.14 holds.

Proof. For an honest user Alice with no input and any dishonest user Bob with output G' we can define a random variable D' such that $D' = \{D'_1 | \dots | D'_{\log k}\}$, where D'_i is Bob's input to the i^{th} $\binom{2}{1}$ -ROT functionality used in the protocol.

Then for all $I = \{I_1 | \dots | I_{\log k}\}$ such that $I \neq D'$, there exists at least one $j \in \{1, \dots, \log k\}$ such that $I_j \neq D'_j$.

Since the $\binom{2}{1}$ -ROTs are secure for Alice for any dishonest user Bob with output G'_j there exists a random variable D'_i such that

$$P_{A_{j,I_j} G'_j A_{j,D'_j} D'_j} \approx_\varepsilon P_U \cdot P_{G'_j A_{j,D'_j} D'_j}. \quad (4.22)$$

Then since $S_{D'} = \bigoplus_{i=1}^{\log k} A_{i,D'_i}$ and $S_I = \bigoplus_{j=1}^{\log k} A_{j,I_j}$ for any $I \neq D'$,

$$P_{S_I G' S_{D'} D'} \approx_{\varepsilon'} P_U \cdot P_{G' S_{D'} D'}, \quad (4.23)$$

where $\varepsilon' \leq \varepsilon \cdot \log k$.

Equation (4.23) proves that Protocol 4.4 is secure for Alice according to Definition 2.14. \square

4.3.2.3 Security For Bob

Finally we show that if the $\binom{2}{1}$ -ROT functionalities are secure for Bob according to Definition 2.9 then Protocol 4.4 is secure for Bob, in the sense of Definition 2.14.

Proof. For an honest user Bob with input $D = \{d_1 | \dots | d_{\log k}\} \in \{1, \dots, k\}$ and any dishonest user Alice we define random variables S'_1, \dots, S'_k in the following way:

$$S'_I = \bigoplus_{j=1}^{\log k} A_{j, I_j}, \text{ for } I \in \{1, \dots, k\}, \quad (4.24)$$

where $A'_{i,0}$ and $A'_{i,1}$ are the inputs in the i^{th} $\binom{2}{1}$ -ROT used in Protocol 4.4.

Then since the $\binom{2}{1}$ -ROTs are secure for Bob there exist random variables $A'_{i,0}, A'_{i,1}$ such that for the output of the i^{th} $\binom{2}{1}$ -ROT

$$P[G_{i, \binom{2}{1}\text{-OT}} = A'_{i, D_i}] \geq 1 - \varepsilon, \quad (4.25)$$

and

$$P_{D_i A'_{i,0} A'_{i,1}} \approx_{\varepsilon} P_{D_i} \cdot P_{A'_{i,0} A'_{i,1}}, \quad (4.26)$$

for all $i = 1, \dots, \log k$.

Since $S_D = \bigoplus_{j=1}^{\log k} A'_{j, D_j}$, (4.25) implies that

$$P[G_{\binom{k}{1}\text{-ROT}} = S'_D] \geq 1 - \varepsilon', \quad (4.27)$$

with $\varepsilon' \leq \varepsilon \cdot \log k$.

Furthermore (4.26) implies that the distribution of D_i is independent of the inputs of that $\binom{2}{1}$ -OT. Since a dishonest user Alice receives no information the choices of Bob are independent. Then since $D = \{D_1 | \dots | D_{\log k}\}$ and $S'_I = \bigoplus_{j=1}^{\log k} A'_{j, I_j}$

$$P_{D S'_1 \dots S'_k} \approx_{\varepsilon'} P_D \cdot P_{S'_1 \dots S'_k} \quad (4.28)$$

□

Thus if the $\binom{2}{1}$ -OT functionalities used are correct, then Protocol 4.4 is secure, this concludes the proof of Theorem 4.5.

Chapter 5

Secure Identification

In this chapter, we aim to construct a protocol that achieves secure password-based identification. In order to do so, we first study existing protocols, namely the protocol proposed in [DFSS07], that achieves secure identification in the bounded quantum storage model.

First, we adapt this protocol to the isolated qubits model by using a $\binom{k}{1}$ -OT functionality. As we have seen in Chapter 4, it is possible to construct a $\binom{k}{1}$ -OT protocol in this model. However, we notice that this identification protocol requires interaction from Bob to Alice.

Secondly, we study if it is possible to construct a non-interactive secure identification protocol. We show that such a protocol is impossible to construct, even based on oblivious transfer.

Finally, we prove the security of an interactive password-based identification protocol that makes use of a $\binom{k}{1}$ -ROT functionality. The latter can be implemented efficiently, as we showed in Chapter 4.

5.1 Secure Identification From $\binom{k}{1}$ -OT

There are a number of secure password-based identification protocols in the literature, we present [DFSS07, Protocol Q-ID] that achieves secure identification in the bounded quantum storage model. Let $c : \mathcal{W} \mapsto \{+, \times\}^n$ be the encoding function, where $+$ is the computational and \times is the Hadamard basis.

Protocol 5.1. *Interactive Password-based Identification with inputs W_A and W_B , the passwords of user Alice and user Bob respectively. Let \mathcal{F} and \mathcal{H} be families of strong 2-universal hash functions [DFSS07]:*

1. *The user Alice picks $x_R \in \{0, 1\}^n$ and $\theta \in_R \{+, \times\}^n$ she then sends state $|x\rangle_\theta$ to Bob*
2. *Bob measures $|x\rangle_\theta$ in basis $D = c(W_B)$. Let X_D be the outcome.*
3. *Alice picks $f \in \mathcal{F}$ uniformly at random and sends θ and f to Bob. Both compute $I_W := \{i : \theta_i = c(W)_i\}$.*
4. *Bob picks $h \in \mathcal{H}$ uniformly at random and sends h to Alice.*

5. Alice sends $z := f(X_{W_A}|_{I_{W_A}}) \oplus h(W_A)$ to Bob, where $X_{W_A}|_{I_{W_A}}$ is the restriction of X_{W_A} to the coordinates X_i with $i \in I_{W_A}$.
6. Bob accepts if and only if $z = f(X_D|_{I_{W_B}}) \oplus h(W_B)$

While this protocol is secure in the bounded-quantum storage model, it is not secure in the isolated qubits model as we have discussed in Chapter 2. Note however that the first part of the protocol (steps 1-4) can be seen as a protocol that implements the $\binom{k}{1}$ -OT functionality. As we have shown in Chapter 4, there exists a protocol that achieves that in the isolated qubits model. Taking this fact into account, we construct a password-based identification protocol that relies on the security of a $\binom{k}{1}$ -OT functionality. A sketch of the protocol is presented in Figure 5.1.

Protocol 5.2. *Password-based identification protocol with inputs W_A and W_B , the passwords of user Alice and user Bob respectively. Let \mathcal{H} be a family of strong 2-universal hash functions such that $h \in \mathcal{H}$ and $h : \{1, \dots, k\} \mapsto \{0, 1\}^\ell$. Then the protocol between Alice and Bob is the following:*

1. The user Alice uses a $\binom{k}{1}$ -OT functionality, $\mathcal{F}_{\binom{k}{1}\text{-OT}}$, with inputs $X_1, X_2, \dots, X_k \in \mathcal{X}$.
2. The user Bob inputs his choice $D = W_B$ to the $\binom{k}{1}$ -OT and receives the message X_D
3. Bob sends a function $h \in \mathcal{H}$ to Alice.
4. Alice sends $z := X_{W_A} \oplus h(W_A)$ to Bob.
5. The user Bob outputs 1 if $z = X_D \oplus h(W_B)$ and 0 otherwise.

In Section 5.3, we will prove the security of a similar protocol that relies on the weaker $\binom{k}{1}$ - $\widetilde{\text{ROT}}$ functionality, that can be implemented efficiently using $\log k$ $\binom{2}{1}$ -ROT functionalities.

Note however, that both Protocol 5.1 and 5.2 use interaction from Bob to Alice. But if we assume that we can implement a $\binom{k}{1}$ -OT functionality securely and non-interactively, can we use it to construct a non-interactive secure identification protocol?

5.2 Impossibility Proof

In this section we study if it is possible to construct a non-interactive password-based identification protocol using a $\binom{k}{1}$ -OT. We introduce a general protocol that uses one instance of the $F_{\binom{k}{1}\text{-OT}}$ functionality to implement the identification functionality F_{ID} and we then prove that such a protocol cannot be secure. We aim to emphasize the importance of the interaction from Bob to Alice (step 4 of Protocol 5.2) in order to implement the identification functionality securely.

5.2.1 Non-Interactive Password-Based Identification

We formally introduce the protocol later (Protocol 5.3), but we first describe it to give some intuition and argue why the protocol is a general form for all such possible protocols. The user Alice has as input a password W_A , can choose inputs X_1, \dots, X_k to the $\binom{k}{1}$ -OT and sends some

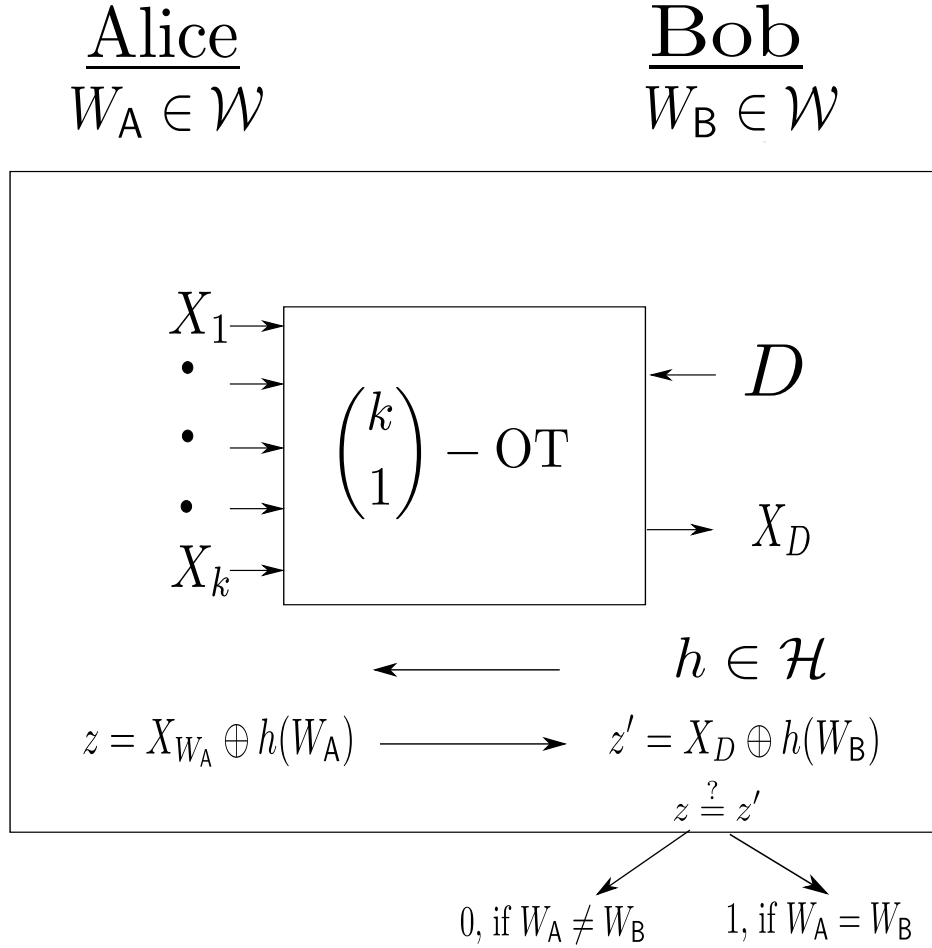


FIGURE 5.1: Sketch of the password-based identification protocol (Protocol 5.2) that makes use of a $\binom{k}{1}$ -OT functionality.

extra information Y to the user Bob depending on the specific protocol. In Protocol 5.2 for example, Y is the function f and the message $z = f(X_{W_A} \oplus h(W_A))$. The user Bob has as input his password W_B and makes a choice regarding the message he will retrieve from the $\binom{k}{1}$ -OT. His choice D may depend on his password so that if his password choice is equal to the choice of Alice he will be able to correctly identify her while he will not be able to do so in any other case. So his choice is described by a deterministic function $c : \mathcal{W} \times \mathcal{Y} \mapsto \{1, \dots, k\}$ such that $D = c(W_B, Y)$ returns the message that when combined with the information Y will allow him to check if $W_A = W_B$.

We note that any non-interactive protocol that uses the $\mathcal{F}_{\binom{k}{1}\text{-OT}}$ functionality once has to be of this form. Since it is non-interactive the user Alice can use the functionality of $\mathcal{F}_{\binom{k}{1}\text{-OT}}$ once and at most send some additional information Y . On the other hand the user Bob receives information Y and can interact with the $\mathcal{F}_{\binom{k}{1}\text{-OT}}$ functionality by inputting his choice D , that can at most depend on both Y and his password choice W_B . Finally, he can, at most, use W_B , D , X_D and Y as inputs to some function g to evaluate the equality function.

Protocol 5.3. *Non-interactive identification protocol with inputs W_A and W_B , the passwords of user Alice and user Bob respectively :*

1. The user Alice uses the non-interactive $\binom{k}{1}$ -OT functionality, $\mathcal{F}_{\binom{k}{1}-OT}$, with inputs $X_1, X_2, \dots, X_k \in \mathcal{X}$ and sends additional information Y to Bob. She chooses the inputs and additional information uniformly at random from a joint distribution $P_{X_1 \dots X_k Y | W_A}$.
2. The user Bob inputs his choice $D = c(W_B, Y)$ to the $\binom{k}{1}$ -OT and receives the message X_D .
3. The user Bob then computes and outputs the acceptance predicate, G :

$$G = g(W_B, X_D, Y) = \begin{cases} 0, & \text{if he rejects,} \\ 1, & \text{if he accepts.} \end{cases} \quad (5.1)$$

A non-interactive identification protocol in this $\binom{k}{1}$ -OT hybrid model is defined by the following ingredients: $P_{Y X_1 \dots X_k | W_A}, P_{D | W_B Y}, P_{G | W_B D X_D Y}$

In order for Protocol 5.3 to be secure it must fulfill the conditions of the security definition Definition 2.16. We consider the special case for $\epsilon = 0$ for perfect security of the protocol. We did not study the case that a non-interactive ϵ -secure password-based identification protocol can be constructed using oblivious transfer. Although studying the $\epsilon > 0$ case remains an interesting problem for future research, we consider the intuition we collect from the following proof (Section 5.2.2) sufficient to emphasise the importance of interaction between Bob and Alice as discussed in Section 5.2.3. This result justifies the use of interaction in the construction of a secure password-based identification protocol, which is the main goal of this thesis.

Then for users Alice and Bob that hold X_1, \dots, X_k, Y and D, X_D, Y, G respectively, we can formulate the following security definition, that is equivalent to Definition 2.16.

Definition 5.4. *The non-interactive identification Protocol 5.3 is secure if the following conditions are fulfilled:*

Correctness: *For honest user Alice and honest user Bob, Bob outputs $G = 1$ if $W_A = W_B$.*

Security for Alice: *For any dishonest user Bob, for any distribution of W_A , there exists a random variable W' that is independent of W_A and such that:*

$$P_{W_A W' Y X_D | W' \neq W_A} = P_{W_A \leftrightarrow W' \leftrightarrow Y X_D | W' \neq W_A} \quad (5.2)$$

Security for Bob: *For any dishonest user Alice, for any distribution of W_B , there exists a random variable W' independent of W_B such that if $W' \neq W_B$ then $P[G = 1 | W_B \neq W'] = 0$, and:*

$$P_{W_B W' Y X_1 \dots X_k | W' \neq W_B} = P_{W_B \leftrightarrow W' \leftrightarrow Y X_1 \dots X_k | W' \neq W_B} \quad (5.3)$$

The following theorem states that it is impossible for a protocol that uses one instance of a $\binom{k}{1}$ -OT functionality to implement the identification functionality securely.

Theorem 5.5. *If Protocol 5.3 is correct and secure for Alice according to Definition 5.4, then it is not secure for Bob.*

5.2.2 Proof Of Theorem 5.5

We first introduce some lemmas that we will use later to prove Theorem 5.5.

Lemma 5.6. *If Protocol 5.3 is secure for Alice then for all $i \in \{1, \dots, k\}$ the joint distribution of the random variables X_i and Y are independent of W_A .*

Proof. Since Protocol 5.3 is secure for Alice, for all P_{W_A} , for all $i \in \{1, \dots, k\}$ there exists W' independent of W_A such that:

$$P_{W_A W' X_i Y, W' \neq W_A} = P_{W_A \leftrightarrow W' \leftrightarrow X_i Y | W' \neq W_A}. \quad (5.4)$$

Then by definition:

$$P_{W_A | W' X_i Y, W' \neq W_A} = P_{W_A | W', W' \neq W_A} \quad (5.5)$$

We also note that trivially when $W' = W_A$,

$$P_{W_A | W' X_i Y, W_A = W'} = P_{W_A | W', W_A = W'} \quad (5.6)$$

Using the property of the marginal distribution:

$$\begin{aligned} P_{W_A | W' X_i Y} &= P[W' \neq W_A] P_{W_A | W' X_i Y, W' \neq W_A} \\ &\quad + P[W' = W_A] P_{W_A | W' X_i Y, W' = W_A} \end{aligned} \quad (5.7)$$

$$\stackrel{(5.5), (5.6)}{=} P[W' \neq W_A] P_{W_A | W', W' \neq W_A} + P[W' = W_A] P_{W_A | W', W' = W_A} \quad (5.8)$$

$$= P_{W_A | W'} \quad (5.9)$$

Using the fact that W' is independent of W_A equation (5.9) becomes:

$$P_{W_A | W' X_i Y} = P_{W_A} \quad (5.10)$$

From equation (5.10) we observe that W', X_i, Y are independent of W_A . □

The next lemma states that if Protocol 5.3 is secure for Alice and correct then the function $c(\cdot, y)$ is injective for all possible y .

Lemma 5.7. *If Protocol 5.3 is correct and secure for Alice then for the function $c : \mathcal{W} \times \mathcal{Y} \rightarrow [k]$ the following holds:*

$$\forall y \in \mathcal{Y} \text{ with } P_Y(y) > 0, \quad c(\cdot, y) \text{ is injective.} \quad (5.11)$$

Proof. Let us assume that the function $c(W_B, Y)$ is not injective.

Then $\exists y : P_Y(y) > 0$ and $\exists j, m \in \mathcal{W}$ with $j \neq m$ such that

$$c(j, y) = c(m, y). \quad (5.12)$$

Then clearly,

$$X_{c(j,y)} = X_{c(m,y)}, \quad (5.13)$$

which immediately implies that,

$$g(j, X_{c(m,y)}, y) \stackrel{(5.14)}{=} g(j, X_{c(j,y)}, y). \quad (5.14)$$

Let us assume that $W_A = j$ and $W_B = m$. Since Protocol 5.3 is correct, Bob computes:

$$g(m, X_{c(m,y)}, Y) = 0, \quad (5.15)$$

but also

$$g(j, X_{c(m,y)}, y) \stackrel{(5.14)}{=} g(j, X_{c(j,y)}, y) = 1. \quad (5.16)$$

This means that for $W_A \neq W_B$, Bob learns the password of Alice and thus

$$P_{W_A W' Y X_D | W' \neq W_A} \neq P_{W_A \leftrightarrow W' \leftrightarrow Y X_D | W' \neq W_A}, \quad (5.17)$$

which means that Protocol 5.3 is not secure for Alice. Thus if Protocol 5.3 is correct and secure for Alice the function $c(W_B, Y)$ is injective. \square

From correctness we expect that for all password inputs $w \in \mathcal{W}$ there exists a $y \in \mathcal{Y}$ and there exists a $x \in \mathcal{X}$ that Alice can input in the $\binom{k}{1}$ -OT and will lead Bob to output $G = g(w, x, y) = 1$. The following lemma states that it must be so for all $y \in \mathcal{Y}$ with $P_Y(y) > 0$, for all password inputs $w \in \mathcal{W}$ simultaneously. Intuitively this is so because otherwise a dishonest user Bob would gain some information on the password of Alice from the message Y . He could for example exclude some password choices after seeing Y , making the protocol insecure for Alice.

Lemma 5.8. *If Protocol 5.3 is correct and secure for Alice, then for all $w \in \mathcal{W}$, for all $y \in \mathcal{Y}$ such that $P_Y(y) > 0$ there exists a $x \in \mathcal{X}$ such that:*

$$g(w, x, y) = 1 \quad (5.18)$$

Proof. We will prove this lemma by contraposition.

Assume that there exists a $w \in \mathcal{W}$ and there exists a $y \in \mathcal{Y}$ with $P_{Y|W_A}(y|w) > 0$ such that for all $x \in \mathcal{X}$:

$$g(w, x, y) = 0 \quad (5.19)$$

Let $W_A = W_B = w$. Then for all $x \in \mathcal{X}$

$$g(w, x, y) = 0, \quad (5.20)$$

which implies that Protocol 5.3 is not correct.

So far we have shown that if Protocol 5.3 is correct, then for all $w \in \mathcal{W}$, for all $y \in \mathcal{Y} : P_{Y|W_A}(y|w) > 0$ there exists a $x \in \mathcal{X}$ such that $g(w, x, y) = 1$.

Furthermore security for Alice implies that $P_{Y|W_A} = P_Y$ via Lemma 5.6 and thus we can conclude that:

For all $w \in \mathcal{W}$ for all $y \in \mathcal{Y}$ with $P_Y(y) > 0$, there exists a $x \in \mathcal{X}$ such that:

$$g(w, x, y) = 1 \quad (5.21)$$

□

Note that on the one hand, the information Y Alice sends does not give any information about her password input, which is necessary to ensure her security. On the other hand, it also means that Alice does not commit to a password choice by sending the information Y to Bob.

We now prove Theorem 5.5 using the above lemmas. The intuition behind the following proof is that if the identification Protocol 5.3 is correct and secure for Alice, a dishonest Bob cannot learn anything about the password of Alice from the output of the $\binom{k}{1}$ -OT X_D or the additional information Y alone except for the output G . He also does not learn anything about the other inputs in the $\binom{k}{1}$ -OT, thus allowing a dishonest user Alice to launch an attack by choosing the inputs to the $\binom{k}{1}$ -OT, X_1, \dots, X_k , such that each one of them combined with Y will force Bob to accept for all of his password choices W_B . Then Protocol 5.3 is clearly not secure for Bob since the dishonest user Alice does not need to choose one password W_A but can force Bob to always accept.

Proof. If Protocol 5.3 is correct and secure for Alice, a dishonest user Alice can use the following attack to force Bob to accept for all of his password choices. Alice inputs $W_A = 1$, chooses a value for Y honestly and then picks the inputs to the $\binom{k}{1}$ -OT, X_1, \dots, X_k , such that for every

password choice W_B of the user Bob, he will obtain $X_i = X_{c(W_B, Y)}$ such that he will output $G = 1$.

Attack Strategy Of Dishonest User Alice

1. Alice chooses $Y = y$ (honestly) according to the distribution $P_{Y|W_A=1}$, and sends it to Bob.
2. Alice uses the non-interactive $\binom{k}{1}$ -OT functionality, with inputs X_1, \dots, X_k that she chooses as follows.

For every password $w \in \mathcal{W}$:

- (a) Find a x such that:

$$P_{X_j|W_A=w, Y=y}(x) > 0, \text{ with } j = c(w, y) \quad (5.22)$$

and

$$G = g(w, x, y) = 1. \quad (5.23)$$

- (b) Set input $X_j = x$, with $j = c(w, y)$.

Note that step 2 is possible because correctness and security for Alice imply, via Lemma 5.8, that for all possible choices of Y and for all possible password choices $w \in \mathcal{W}$ there exists a $x \in \mathcal{X}$ such that $G = 1$.

Furhtermore, Lemma 5.7 implies that the function $c(W_B, y)$ is injective for all $y \in \mathcal{Y}$. Then once y is chosen, for every $w \in \mathcal{W}$ there exists only one $j \in \{1, \dots, k\}$, such that $j = c(w, y)$.

These two facts allow a dishonest Alice to choose the inputs of the $\binom{k}{1}$ -OT, such that for every password choice of Bob $w \in \mathcal{W}$ he retrieves a $x \in \mathcal{X}$ such that he outputs $G = 1$.

In more detail, after receiving the $\binom{k}{1}$ -OT and $Y = y$, the honest user Bob chooses a password W_B , inputs his choice $D = c(W_B, y)$ to the $\binom{k}{1}$ -OT and receives the message X_D . As described above for every one of his password choices he receives a message $X_D = x$ such that $g(w, x, y) = 1$. He then outputs $G = g(W_B, X_D, Y) = 1$ for any of his password choices, which implies that Protocol 5.3 is not secure for Bob.

□

5.2.3 The Importance Of Interaction

Theorem 5.5 shows that a non-interactive protocol using one instance of a $\binom{k}{1}$ -OT functionality cannot implement the identification functionality securely. We proved that security for Alice and correctness of the protocol allow the attack described above to succeed and we claim that this is true as long as Alice has knowledge of the function $g(W_B, X_D, Y)$. This knowledge allows her to choose the inputs to the $\binom{k}{1}$ -OT such that Bob will accept for all of his passwords, making the protocol insecure.

It is then interesting to examine where (interactive) protocols that are known to be secure differ. In the examples of [DFSS07, Protocol Q-ID] and Protocol 5.2 the user Bob sends some information to Alice after receiving the $\binom{k}{1}$ -OT, in this case a strong 2-universal hash function. This interaction makes the protocol secure for Bob against the above attack, because the (possibly extended) function $g(W_B, X_D, Y)$ as defined above, is fixed after Alice has chosen her inputs to the $\binom{k}{1}$ -OT. Fixing the function g after Alice has committed to her inputs to the $\binom{k}{1}$ -OT denies her the possibility to choose them in such a way that $G = 1$ for all passwords. Thus we conclude that as long as the function that is used by Bob to determine the acceptance predicate is fixed before Alice chooses her inputs to the $\binom{k}{1}$ -OT, she can choose the inputs such that the above attack will work.

Extending the non-interactive Protocol 5.3 by allowing multiple uses of the $\binom{k}{1}$ -OT functionality, or even $\binom{k}{b}$ -OT functionalities from Alice to Bob will still be insecure for Bob as the function $g(\cdot)$ is fixed before Alice chooses her inputs to the $\binom{k}{1}$ -OTs. For the same reason, an interaction from Bob to Alice before she chooses her inputs to the $\binom{k}{1}$ -OT would not stop the above attack from functioning.

5.3 Secure Identification From $\binom{k}{1}$ - $\widetilde{\text{ROT}}$ With Interaction

In Section 5.1 we introduced Protocol 5.2, a password-based identification protocol based on a $\binom{k}{1}$ -OT functionality. The $\binom{k}{1}$ -OT construction we showed in Chapter 4 is, however, inefficient as it requires k instances of an $\binom{2}{1}$ -OT functionality, where k is the number of passwords.

In this section, we show that one can instead use the $\binom{k}{1}$ - $\widetilde{\text{ROT}}$ functionality that only requires $\log k$ $\binom{2}{1}$ -OTs. While weaker than the $\binom{k}{1}$ -OT or $\binom{k}{1}$ -ROT functionalities, it is sufficient to achieve security for the password-based identification protocol.

We introduce the password-based identification protocol that relies on the security of a $\binom{k}{1}$ - $\widetilde{\text{ROT}}$ functionality. A sketch of the protocol is shown in Figure 5.2

Protocol 5.9. *Password-based identification protocol with inputs $W_A, W_B \in \mathcal{W}$, the passwords of user Alice and user Bob respectively, where $\mathcal{W} = \{1, \dots, k\}$. Let \mathcal{H} be a family of strong 2-universal hash functions such that $h \in \mathcal{H}$ and $h : \mathcal{W} \mapsto \{0, 1\}^\ell$. Then the protocol between Alice and Bob is the following:*

1. The users Alice and Bob employ a $\binom{k}{1}$ - $\widetilde{\text{ROT}}$ functionality, $\mathcal{F}_{\binom{k}{1}-\widetilde{\text{ROT}}}$ that takes no input from Alice and input $D \in \mathcal{W}$ from Bob.
2. The user Alice receives outputs $S_1, S_2, \dots, S_k \in \mathcal{S}$ and Bob receives output string $S_D \in \mathcal{S}$, where $\mathcal{S} = \{0, 1\}^\ell$.
3. Bob chooses a function $h \in \mathcal{H}$ uniformly at random and sends h to Alice.
4. Alice sends $z := S_{W_A} \oplus h(W_A)$ to Bob.
5. The user Bob accepts if and only if $z = S_D \oplus h(W_B)$.

We now introduce a theorem that states that the secure identification protocol we propose above is secure in the sense of Definition 2.16 if the $\binom{k}{1}$ - $\widetilde{\text{ROT}}$ functionality used is secure according to Definition 2.13.

Theorem 5.10. *If there exists a protocol that implements the $\binom{k}{1} - \widetilde{\text{ROT}}$ functionality ε -securely according to Definition 2.14 and the min-entropy of password choices W is $H_{\min}(W) \geq 1$, then Protocol 5.9 is ε' -secure in the sense of Definition 2.16, where $\varepsilon' = \varepsilon + \frac{k^2}{2^\ell}$.*

In Chapter 4 we have showed how to construct a secure $\binom{k}{1} - \widetilde{\text{ROT}}$ protocol relying on a secure $\binom{2}{1} - \text{ROT}$. Moreover, in Chapter 3 we have showed that a secure $\binom{2}{1} - \text{ROT}$ protocol exists in the isolated qubits model. Taking these results into account, the previous theorem states that our password-based identification protocol is secure in the isolated qubits model.

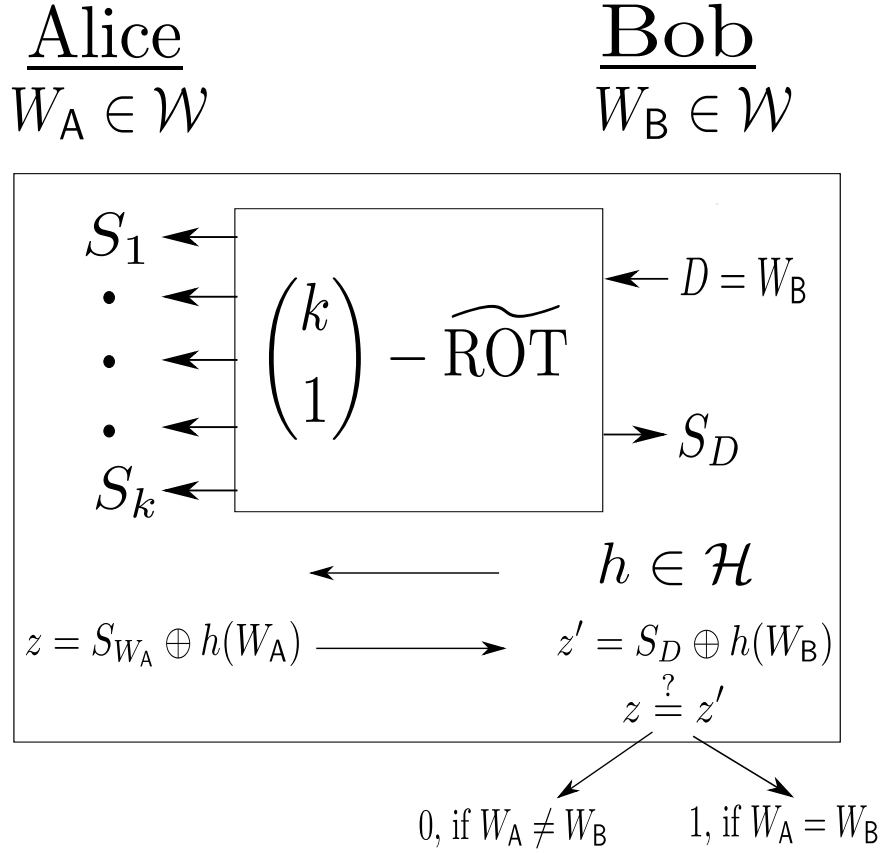


FIGURE 5.2: Sketch of the password-based identification protocol (Protocol 5.9) that makes use of a $\binom{k}{1} - \widetilde{\text{ROT}}$ functionality.

5.3.1 Proof Of Theorem 5.10

Finally, in this section, we prove that if the $\binom{k}{1} - \widetilde{\text{ROT}}$ used in Protocol 5.9 is secure then the identification protocol is secure.

5.3.1.1 Correctness

Proof. Honest users Alice and Bob hold inputs W_A and W_B .

Following Protocol 5.9 Bob inputs $D = W_B$ in the $\binom{k}{1} - \widetilde{\text{ROT}}$ functionality which is correct and thus Bob receives output

$$G_{\binom{k}{1} - \widetilde{\text{ROT}}} = S_D = S_{W_B}, \quad (5.24)$$

except with probability ε .

Then $z' = S_D \oplus h(W_B) = S_{W_B} \oplus h(W_B)$.

Since Alice is honest $z = S_{W_A} \oplus h(W_A)$ and thus if $W_A = W_B$ then $z = z'$ and Bob will output $G = 1$.

Similarly if $W_A \neq W_B$ Bob will output $G = 0$ except with probability $\frac{k^2}{2^\ell}$, the probability that $h(W_A) = h(W_B)$ given $W_A \neq W_B$.

Thus Protocol 5.9 is correct except with probability $\varepsilon' = \varepsilon + \frac{k^2}{2^\ell}$.

□

5.3.1.2 Security For Alice

Proof. For honest user Alice with input W_A and any dishonest user Bob we can define a random variable $W' = D'$, where D' is Bob's input in the $\binom{k}{1} - \widetilde{\text{ROT}}$ used in the protocol. Since Bob has received no information before he decides on his input to the $\binom{k}{1} - \widetilde{\text{ROT}}$, D' and thus W' are independent of the input W_A that honest Alice holds.

Furthermore W_A is independent of the messages S_1, \dots, S_k that Alice receives from the $\binom{k}{1} - \widetilde{\text{ROT}}$ since she has chosen it before receiving any output from the $\binom{k}{1} - \widetilde{\text{ROT}}$ and the latter takes no input from Alice.

From the above it is clear that if $W' \neq W_A$ and since $W' = D'$ then

$$P_{W_A W' S_{W'} | W' \neq W_A} = P_{W_A \leftrightarrow W' \leftrightarrow S_{W'} | W' \neq W_A}. \quad (5.25)$$

Furthermore from the security of $\binom{k}{1} - \widetilde{\text{ROT}}$, there exists a random variable D' such that for all $I \neq D'$ the following holds

$$P_{S_I D' S_{D'} | D' \neq I} \approx_\varepsilon P_U \cdot P_{D' S_{D'} | D' \neq I}. \quad (5.26)$$

Then for $I = W_A$ and $W_A \neq W'$ equation (5.26) becomes,

$$P_{S_{W_A} W' S_{W'} | W' \neq W_A} \approx_\varepsilon P_U \cdot P_{W' S_{W'} | W' \neq W_A}. \quad (5.27)$$

Consider the random variable $Z = S_{W_A} \oplus h(W_A)$ that describes the message Alice sends to Bob after receiving the hash function h . Taking into account that W_A is independent of W', D' and S_1, \dots, S_k , including $S_{W'}$ and S_{W_A} , conditioned on the event $W' \neq W_A$. Then from the properties of the modulo 2 addition and equation (5.27) we have that

$$P_{ZW_A W' S_{W'} | W' \neq W_A} \approx_\varepsilon P_U \cdot P_{W_A W' S_{W'} | W' \neq W_A}. \quad (5.28)$$

From equation (5.25) the above can be written as:

$$P_{ZW_A W' S_{W'} | W' \neq W_A} \approx_\varepsilon P_U \cdot P_{W_A \leftrightarrow W' \leftrightarrow S_{W'} | W' \neq W_A} \quad (5.29)$$

$$\approx_\varepsilon P_{W_A \leftrightarrow W' \leftrightarrow Z S_{W'} | W' \neq W_A} \quad (5.30)$$

$$\approx_{\varepsilon'} P_{W_A \leftrightarrow W' \leftrightarrow Z S_{W'} | W' \neq W_A}, \quad (5.31)$$

with $\varepsilon' = \varepsilon + \frac{k^2}{2^\ell}$.

Then Protocol 5.9 is ε' -secure for Alice. \square

5.3.1.3 Security For Bob

Proof. Since the $\binom{k}{1} - \widetilde{\text{ROT}}$ functionality, that is implemented by an honest user Bob with input $D = W_B$ and a dishonest user Alice, is secure for Bob, there exist random variables S'_1, \dots, S'_k such that

$$P_{DV' S'_1 \dots S'_k} \approx_\varepsilon P_D \cdot P_{V' S'_1 \dots S'_k}. \quad (5.32)$$

It is clear that V', S'_1, \dots, S'_k are independent of W_B .

We then define $Z_i = S'_i \oplus h(i)$ for $i \in \mathcal{W}$. Consider the event \mathcal{E} that all Z_i 's are distinct. Since h is strong 2-universal and is also independent of S'_i the Z_i 's are pairwise independent. Then from the union bound it follows that the event \mathcal{E} occurs except with probability $k(k-1)/2 \cdot 1/2^\ell \leq k^2/2^{\ell+1}$.

We define random variable W' such that the message sent by Alice $Z = S_{W'} \oplus h(W')$. If $Z \neq Z_i$ for all i then we set $W' = \perp$ and honest Bob always outputs $G = 0$ regardless of his password choice W_B . In this case a dishonest user Alice learns nothing about W_B . Similarly from the way that W' is defined Bob will output $G = 1$ if $W' = W_B$.

Note that from security of the $\binom{k}{1} - \widetilde{\text{ROT}}$ functionality, and since h is picked uniformly at random, W' is independent of W_B . This further implies that Z_1, \dots, Z_k, Z are also independent of W_B . Moreover since the event \mathcal{E} is determined by the Z_i 's it also holds that Z_1, \dots, Z_k, Z are independent from W_B conditioned on the event \mathcal{E} and even given W' conditioned on \mathcal{E} and $W' \neq W_B$.

Now consider Z_1, \dots, Z_k, Z, G , if $W' \neq W_B$ and event \mathcal{E} then Bob outputs $G = 0$ with probability $P[G = 0 | W' \neq W_B, \mathcal{E}] = 1$. Then Z_1, \dots, Z_k, Z, G are independent of W_B given W' conditioned on the event $W' \neq W_B$ and \mathcal{E} , that is:

$$P_{W_B W' Z_1 \dots Z_k Z G | W' \neq W_B, \mathcal{E}} \approx_{\varepsilon} P_{W_B \leftrightarrow W' \leftrightarrow Z_1 \dots Z_k Z G | W' \neq W_B, \mathcal{E}}. \quad (5.33)$$

We then define $p = P[\mathcal{E} | W' \neq W_B]$ and $\bar{p} = P[\bar{\mathcal{E}} | W' \neq W_B]$. Note that $P[\bar{\mathcal{E}}] \leq k^2/2^{\ell+1}$.

Furthermore since $H_{\min}(W) \geq 1$ it is easy to see that $P[W' = W_B] \leq \frac{1}{2}$. Then

$$\bar{p} = P[\bar{\mathcal{E}} | W' \neq W_B] = \frac{P[\bar{\mathcal{E}}]}{1 - P[W' = W_B]} \leq 2P[\bar{\mathcal{E}}] \leq \frac{k^2}{2^{\ell}}. \quad (5.34)$$

Note that \bar{p} upperbounds the probability $P[G = 1 | W' \neq W_B] \leq \bar{p} \leq \frac{k^2}{2^{\ell}} \leq \varepsilon'$, where $\varepsilon' = \varepsilon + \frac{k^2}{2^{\ell}}$, fulfilling the first condition for security.

From basic probability theory and using equation (5.33) :

$$P_{W_B W' Z'_1 \dots Z'_k Z G | W' \neq W_B} = p \cdot P_{W_B W' Z'_1 \dots Z'_k Z G | W' \neq W_B, \mathcal{E}} + \bar{p} \cdot P_{W_B W' Z'_1 \dots Z'_k Z G | W' \neq W_B, \bar{\mathcal{E}}} \quad (5.35)$$

$$\approx_{\varepsilon} p \cdot P_{W_B \leftrightarrow W' \leftrightarrow Z'_1 \dots Z'_k Z G | W' \neq W_B, \mathcal{E}} + \bar{p} \cdot P_{W_B W' Z'_1 \dots Z'_k Z G | W' \neq W_B, \bar{\mathcal{E}}} \quad (5.36)$$

Finally note that \mathcal{E} is independent of W_B and W' and thus also when conditioned on $W' \neq W_B$, then from conditional independence

$$P_{W_B \leftrightarrow W' \leftrightarrow Z'_1 \dots Z'_k Z G | W' \neq W_B} = p \cdot P_{W_B \leftrightarrow W' \leftrightarrow Z'_1 \dots Z'_k Z G | W' \neq W_B, \mathcal{E}} + \bar{p} \cdot P_{W_B \leftrightarrow W' \leftrightarrow Z'_1 \dots Z'_k Z G | W' \neq W_B, \bar{\mathcal{E}}}. \quad (5.37)$$

The distance between two probability distributions is upper-bounded by one by definition. Then so is the distance between $P_{W_B W' Z'_1 \dots Z'_k Z G | W' \neq W_B, \bar{\mathcal{E}}}$ and $P_{W_B \leftrightarrow W' \leftrightarrow Z'_1 \dots Z'_k Z G | W' \neq W_B, \bar{\mathcal{E}}}$.

Thus the distance between $P_{W_B W' Z'_1 \dots Z'_k Z G | W' \neq W_B}$ and $P_{W_B \leftrightarrow W' \leftrightarrow Z'_1 \dots Z'_k Z G | W' \neq W_B}$ is upper-bounded by $\bar{p} + \varepsilon \leq k^2/2^{\ell} + \varepsilon = \varepsilon'$.

Then since Alice's output V' is defined by Z_1, \dots, Z_k, Z, G :

$$P_{W_B W' V' | W' \neq W_B} \approx_{\varepsilon'} P_{W_B \leftrightarrow W' \leftrightarrow V' | W' \neq W_B}. \quad (5.38)$$

Thus Protocol 5.9 is secure for Bob. □

Thus Protocol 5.9 is secure. We note that this protocol is more efficient than the previous identification protocols, because of the more efficient construction of $\binom{k}{1}$ – $\widetilde{\text{ROT}}$ compared to the $\binom{k}{1}$ – ROT protocol presented in Chapter 4.

Chapter 6

Conclusions & Discussion

In this final chapter, we summarise our main results and conclusions. Then we open the discussion of these results in relation to current knowledge. Finally, we pose some of the questions that arise from this discussion and propose possible future steps.

6.1 Conclusions & Discussion

In Chapter 3 we presented a secure string $\binom{2}{1}$ -ROT in the isolated qubits model, using the “leaky” OTM presented in [Liu14b]. We note that our proof follows a similar path to the one used in [Liu15], but makes use of the notion of non-degenerate linear functions coupled with the results of [DFSS06]. The resulting proof is simpler than the original and allows us to construct a secure string $\binom{2}{1}$ -ROT in the IQM. This comes at a cost, by using Theorem 3.5 security is achieved with an error $2^{2\ell'+1}$ times larger than the one presented in [Liu15]. Fortunately, as shown in equation (3.96), this factor does not influence the security result. However, Theorem 3.3 implies that the security parameter k has to be of the order of ℓ' in order for the protocol to achieve security.

In Chapter 4 we made the first attempt to study more complex two-party functionalities in this model. We propose secure $\binom{2}{1}$ -OT, $\binom{k}{1}$ -OT and $\widetilde{\binom{k}{1}}$ -ROT protocols that rely on the security and composability of an $\binom{2}{1}$ -ROT functionality. In order to guarantee composability of the $\binom{2}{1}$ -ROT protocol, we restricted the users to measure at the end of each protocol. These protocols can then be implemented in the isolated qubits model using an $\binom{2}{1}$ -ROT protocol that is secure in that model, such as Protocol 3.1 presented in Chapter 3.

The question that then arises is if the aforementioned assumption is realistic. Since composability of protocols has not been studied in the isolated qubits this questions remains an open problem for further study and we will briefly discuss this in the next section.

Following that, in Chapter 5 we address an interesting problem of secure two-party computation, the evaluation of the equality function. We present a protocol for secure password-based identification that uses a $\widetilde{\binom{k}{1}}$ -ROT functionality, motivated by the protocols proposed in [DFSS07]. However, the results of Chapter 4 and Chapter 5 are not limited by the specific cryptographic model, they can be implemented in any model in which there exists a protocol that implements the $\binom{2}{1}$ -ROT functionality securely and in a composable way.

An interesting question that we encountered on the way is if it is possible to construct non-interactive secure password-based identification protocols. In Section 5.2, we proved constructing such a protocol based on oblivious transfer is impossible. The interaction from Bob to Alice must define the way he computes his output in order for the protocol to be secure against the attack we presented in Section 5.2.

Moreover, we claim that this result is not restricted to the secure evaluation of the equality function but also applies to more (or even all) secure-function-evaluation problems. For example in the similar problem of Yao's millionaire problem where Bob computes a different function, a dishonest user Alice still has the ability to predetermine the output for all of her inputs, as long as Bob's function is not determined after she has committed to her inputs.

6.2 Future Work

This thesis studies the construction of a secure string $\binom{2}{1}$ -OT protocol if the users are restricted to operations on single qubits and classical communication between them and gives examples of possible applications to construct more complex secure two-party computation protocols such as password-based identification. This leads of course to new questions that remain an open challenge for the future.

As we mentioned in the last section, studying if composability holds in the IQM is likely the most interesting problem that arises from this thesis. If it is shown to be so, we have shown that a secure $\binom{2}{1}$ -OT construction is possible in the IQM, which would imply that any secure two-party computation functionality can be implemented. If however composability does not hold in the IQM, then constructing and analysing protocols in this model would prove an exciting challenge in itself. For example, the problem of analysing the security of two parallel $\binom{2}{1}$ -OTs and modelling the measurement strategies of an adversary who is allowed to partially measure qubits from the first and second $\binom{2}{1}$ -OT and adapt his measurement strategy depending on partial results of each $\binom{2}{1}$ -OT seems to be a first challenge for further research.

As we have already described in Chapter 1 there are numerous results that prove the impossibility of oblivious transfer in a fully quantum world. Nevertheless, there exist different approaches to restrict the users in a realistic fashion and achieve oblivious transfer. One of the most interesting questions that arises from this train of thought is to find the minimal and most realistic restrictions or assumptions needed to achieve secure $\binom{2}{1}$ -OTs. For example, Liu has the question of allowing a number of entangling operations on the isolated qubits in [Liu15], which could be a possible approach to generalise the isolated qubits model.

We have discussed in more detail two approaches to limit an adversary, restricting him to single-qubit operations or restricting his qubit-storage capacity. So far, existing protocols that are secure against one type of adversary are not secure against the other. The question then is, could we construct protocols that combine the power of these two models? For example using a $\binom{2}{1}$ -OT that is secure in the IQM and one that is secure in the noisy-storage model to construct one $\binom{2}{1}$ -OT that is secure in both models and using the modulo 2 addition of their outputs? This would then mean that the adversary would need to both have larger qubit storage capacities, in order to break the noisy-storage model $\binom{2}{1}$ -OT security and be able to perform entangling operations on the qubits he receives, in order to break the isolated qubits model $\binom{2}{1}$ -OT security.

As a further approach to combine these models, Liu has addressed the question of allowing a number of entangling operations on the isolated qubits in [Liu15]. This could be the first step to define a more general model and should be investigated further.

One further possibility for future endeavours that arises from our impossibility proof in Section 5.2.2 is to examine if our result indeed applies to more non-interactive two-party protocols. However, there exist results that state that quantum one-time programs can be constructed from one-time memories [?]. We conjecture that there is a lower-bound on the number of one-time memories needed to construct a secure one-time program for password-based identification so that both results hold. Unfortunately we did not study this into more detail in this thesis and we leave it as an open question.

Furthermore, we leave the task of extending the impossibility proof to the error case as discussed in Section 5.2.1 as an open problem for the future. Our intuition is that the attack described in the proof should function since interaction from Bob to Alice seems to be necessary to achieve security for Bob. Nevertheless formalising this intuition is an interesting extension of the impossibility proof discussed in this thesis.

Appendix A

Probability Theory

A.1 Probability Theory

A.1.1 Random Variables

The probability distribution of a random variable X that takes values $x \in \mathcal{X}$ is a function $P_X : \mathcal{X} \mapsto [0, 1]$ and is defined as:

$$P_X(x) := P[X = x], \forall x \in \mathcal{X} \quad (\text{A.1})$$

Note that for every probability distribution the following holds:

$$\sum_{x \in \mathcal{X}} P_X(x) = 1 \quad (\text{A.2})$$

The joint probability distribution of two random variables X and Y that take values $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ respectively, is defined as:

$$P_{XY}(x, y) := P[X = x, Y = y], \quad (\text{A.3})$$

and indicates the probability that X takes the value x and Y takes the value y simultaneously.

Let P_{XY} be the joint distribution of random variables X and Y . Then the distribution of X can be obtained by marginalising over Y . The distribution P_X is then called a marginal distribution:

$$P_X(x) = \sum_{y \in \mathcal{Y}} P_{XY}(x, y) \quad \forall x \in \mathcal{X}. \quad (\text{A.4})$$

Let P_{XY} be the joint of random variables X and Y . If X and Y are *independent* random variables the joint distribution can be written as:

$$P_{XY}(x, y) = P_X(x) \cdot P_Y(y) \quad \forall x \in \mathcal{X}, \quad \forall y \in \mathcal{Y}. \quad (\text{A.5})$$

Furthermore, the *conditional probability distribution* of a random variable X takes the value $x \in \mathcal{X}$ given the event that the random variable Y takes the value $y \in \mathcal{Y}$ is defined as:

$$P_{X|Y}(x|y) := \frac{P_{XY}(x, y)}{P_Y(y)}. \quad (\text{A.6})$$

Moreover we introduce the symbol $P_{X \leftrightarrow Y \leftrightarrow Z}$, as used in [DFSS07] and [FS09], to denote that the distribution of a random variable X is independent of a random variable Z given a random variable Y :

$$P_{X|YZ} = P_{X|Y} \quad (\text{A.7})$$

Then we write:

$$P_{XYZ} = P_{X \leftrightarrow Y \leftrightarrow Z} \quad (\text{A.8})$$

This notation is extended to $P_{XYZ|\mathcal{E}} = P_{X \leftrightarrow Y \leftrightarrow Z|\mathcal{E}}$ to denote that the distribution of a random variable X is independent of a random variable Z given a random variable Y conditioned on an event \mathcal{E} :

$$P_{X|YZ\mathcal{E}} = P_{X|Y\mathcal{E}} \quad (\text{A.9})$$

Boole's inequality The union bound or Boole's inequality states that the probability of at least one event occurring cannot be greater than the sum of the probabilities of all individual events.

Formally for a set of events A_1, A_2, \dots the following inequality holds:

$$P\left(\bigcup_i A_i\right) \leq \sum_i P(A_i) \quad (\text{A.10})$$

Finally, the expected value of a random variable X that takes values $x \in \mathcal{X}$ is defined as:

$$\mathbb{E}(x) = \sum_{x \in \mathcal{X}} x \cdot P_X(x) \quad (\text{A.11})$$

A.1.2 Uniform Distribution

If a random variable X is uniformly distributed it means that all of its values are equiprobable.

Definition A.1. *A random variable X that takes values $x \in \mathcal{X}$ is uniformly distributed if its distribution P_X is of the following form:*

$$P_X(x) = \frac{1}{|\mathcal{X}|} \quad \forall x \in \mathcal{X} \quad (\text{A.12})$$

Then P_X is a uniform distribution over \mathcal{X} .

A.1.3 ϵ -Net

Intuitively an ϵ -net is a subset of some normed space such that for every point of the original space there is some point in the ϵ -net that is ϵ -close to it. We now introduce the formal definition of an ϵ -net.

Definition A.2. *Let E be a subset of some normed space, with norm $\|\cdot\|$ and let $\epsilon > 0$. Then \tilde{E} is an ϵ -net for E if $\tilde{E} \subset E$, and for all $x \in E$, there exists some $y \in \tilde{E}$ such that:*

$$\|x - y\| \leq \epsilon \quad (\text{A.13})$$

Appendix B

Measures of Uncertainty

B.1 Renyi Entropy

Definition B.1. For a random variable X that takes values $x \in \mathcal{X}$, for $\alpha \in \mathbb{R}$ with $\alpha \geq 0$ and $\alpha \neq 1$, the Renyi entropy of order α is defined as

$$H_\alpha(X) := \frac{1}{1-\alpha} \log \left(\sum_{x \in \mathcal{X}} P_X(x)^\alpha \right) \quad (\text{B.1})$$

We note that the Renyi entropy is a generalised entropy.

For $\alpha = 1$ we obtain the Shannon entropy:

$$H_1(X) := - \sum_{x \in \mathcal{X}} P_X(x) \log(P_X(x)) \quad (\text{B.2})$$

For $\alpha = 0$ we obtain the max-entropy:

$$H_0(X) := \log |\mathcal{X}| \quad (\text{B.3})$$

B.2 Min-Entropy

One important measure of uncertainty for information theory is the Renyi entropy we get for $\alpha \rightarrow \infty$, namely the min-entropy:

$$H_\infty(X) := \min_{x \in \mathcal{X}} [-\log P_X(x)] \quad (\text{B.4})$$

It is the smallest of the Renyi entropies of order α and thus the most conservative estimate of uncertainty in a random variable. This is the reason why it is widely used in cryptography.

Similarly one can define the conditional min-entropy

$$H_\infty(X|Y) := \min_{x \in \mathcal{X}, y \in \mathcal{Y}} [-\log P_{X|Y}(x|y)] \quad (\text{B.5})$$

B.3 Smoothed Min-Entropy

The smoothed min-entropy defined below can be understood as the entropy of a distribution P_X that is smoothed by cutting a probability mass ε from the largest probabilities.

$$H_\infty^\varepsilon(X) := \max_{\mathcal{E}: P(\mathcal{E}) \geq 1-\varepsilon} \min_{x \in \mathcal{X}} [-\log P_X(x)] \quad (\text{B.6})$$

Informally one can think of it as the maximum min-entropy available in any distribution that is ε -close to the distribution P_X .

Furthermore the smoothed conditional min-entropy is defined as:

$$H_\infty^\varepsilon(X|Y) := \max_{\mathcal{E}: P(\mathcal{E}) \geq 1-\varepsilon} \min_{x \in \mathcal{X}, y \in \mathcal{Y}} [-\log P_{X|Y}(x|y)] \quad (\text{B.7})$$

The latter is an important measure in cryptography as it defines the maximum amount of randomness that is available from X given Y and S , except with probability ε .

Appendix C

Linear Algebra

C.1 Norms

For any matrix $A \in \mathbb{C}^{m \times n}$ and vector $x \in \mathbb{C}^n$ we define the following norms:

Operator norm

$$\|A\| = \max_{\|x\|=1} \|Ax\| \quad (\text{C.1})$$

Trace norm

$$\|A\|_{\text{tr}} = \text{tr}(\sqrt{AA^\dagger}) \quad (\text{C.2})$$

Statistical Distance Let P and Q be two probability distributions of a random variable X that takes values $x \in \mathcal{X}$. Then the ℓ_1 distance between them is defined as:

$$\|P - Q\| = \sum_x |P(x) - Q(x)|. \quad (\text{C.3})$$

This is commonly called the statistical distance and is used as a distance measure between the two probability distributions.

Bibliography

- [BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.
- [BBCS92] C. H. Bennett, G. Brassard, C. Crépeau, and M. H. Skubiszewska. Practical Quantum Oblivious Transfer. *Lect. Notes Comput. Sci.*, 576: 351–366, 1992.
DOI: [10.1007/3-540-46766-1_29](https://doi.org/10.1007/3-540-46766-1_29).
- [BBD09] D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post-Quantum Cryptography*, volume 5299. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
DOI: [10.1007/978-3-540-88702-7](https://doi.org/10.1007/978-3-540-88702-7).
- [BBE92] C. H. Bennett, G. Brassard, and A. K. Ekert. Quantum Cryptography, 1992.
DOI: [10.1038/scientificamerican1092-50](https://doi.org/10.1038/scientificamerican1092-50).
- [BC91] G. Brassard and C. Crépeau. Quantum Bit Commitment and Coin Tossing Protocols. In *Advances in Cryptology - CRYPTO 1990*, LNCS, pages 49–61. Springer, 1991.
DOI: [10.1007/3-540-38424-3_4](https://doi.org/10.1007/3-540-38424-3_4).
- [BCJL93] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *34th Annual Foundations of Computer Science - FOCS 1993*, pages 362–371. IEEE, 1993.
DOI: [10.1109/SFCS.1993.366851](https://doi.org/10.1109/SFCS.1993.366851).
- [BCR86] G. Brassard, C. Crepeau, and J.-M. Robert. Information theoretic reductions among disclosure problems. *27th Annu. Symp. Found. Comput. Sci. (sfcs 1986)*, 1986.
DOI: [10.1109/SFCS.1986.26](https://doi.org/10.1109/SFCS.1986.26).
- [BCS12] H. Buhrman, M. Christandl, and C. Schaffner. Complete Insecurity of Quantum Protocols for Classical Two-Party Computation. *Phys. Rev. Lett.*, 109(16): 160501, 2012.
DOI: [10.1103/PhysRevLett.109.160501](https://doi.org/10.1103/PhysRevLett.109.160501).
- [Bra06] G. Brassard. Brief History of Quantum Cryptography: A Personal Perspective. page 14, 2006.
arXiv: [quant-ph/0604072](https://arxiv.org/abs/quant-ph/0604072).
- [Col07] R. Colbeck. Impossibility of secure two-party classical computation. *Physical Review A*, 76(6), 2007.
DOI: [10.1103/physreva.76.062308](https://doi.org/10.1103/physreva.76.062308).
- [Cré88] C. Crépeau. Equivalence Between Two Flavours of Oblivious Transfers. In *Lect. Notes Comput. Sci.*, volume 293, pages 350–354. 1988.
DOI: [10.1007/3-540-48184-2_30](https://doi.org/10.1007/3-540-48184-2_30).

- [Cr 94] C. Cr peau. Quantum Oblivious Transfer. 41(12): 2445–2454, 1994.
DOI: [10.1080/09500349414552291](https://doi.org/10.1080/09500349414552291).
- [DFSS06] I. B. Damg rd, S. Fehr, L. Salvail, and C. Schaffner. Oblivious Transfer and Linear Functions. In *Adv. Cryptol. - CRYPTO 2006, Lect. Notes Comput. Sci.*, volume 4117, pages 427–444. 2006.
DOI: [10.1007/11818175_26](https://doi.org/10.1007/11818175_26).
- [DFSS07] I. B. Damg rd, S. Fehr, L. Salvail, and C. Schaffner. Secure Identification and QKD in the Bounded-Quantum-Storage Model. In *Advances in Cryptology - CRYPTO 2007*, LNCS, pages 342–359. Springer, 2007.
DOI: [10.1007/978-3-540-74143-5_19](https://doi.org/10.1007/978-3-540-74143-5_19).
- [DFSS08] I. B. Damg rd, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the Bounded-Quantum-Storage Model. *SIAM Journal on Computing*, 37(6): 1865–1890, 2008.
DOI: [10.1137/060651343](https://doi.org/10.1137/060651343).
- [EGL85] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. 28(6): 637–647, 1985.
DOI: [10.1145/3812.3818](https://doi.org/10.1145/3812.3818).
- [Eke91] A. K. Ekert. Quantum cryptography based on bell’s theorem. *Physical Review Letters*, 67: 661–663, 1991.
DOI: [10.1103/PhysRevLett.67.661](https://doi.org/10.1103/PhysRevLett.67.661).
- [FS09] S. Fehr and C. Schaffner. Composing Quantum Protocols in a Classical Environment. In *Theory Cryptogr.*, volume 5444 LNCS, pages 350–367. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
DOI: [10.1007/978-3-642-00457-5_21](https://doi.org/10.1007/978-3-642-00457-5_21).
- [Kah96] D. Kahn. *The Codebreakers: The story of secret writing*. Scribner, New York, 1996.
Online: https://www.goodreads.com/book/show/29608.The_Codebreakers.
- [Kil88] J. Kilian. Founding Cryptography on Oblivious Transfer. *Proc. 20th Annu. ACM Symp. Theory Comput.*, pages 20–31, 1988.
DOI: [10.1145/62212.62215](https://doi.org/10.1145/62212.62215).
- [KL07] J. Katz and Y. Lindell. *Introduction to Modern Cryptography*. 2007.
DOI: [10.1080/10658989509342477](https://doi.org/10.1080/10658989509342477).
- [KWW12] R. K nig, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3): 1962–1984, 2012.
DOI: [10.1109/TIT.2011.2177772](https://doi.org/10.1109/TIT.2011.2177772).
- [LC97] H.-K. Lo and H. Chau. Is Quantum Bit Commitment Really Possible? *Physical Review Letters*, 78(17): 3410–3413, 1997.
DOI: [10.1103/PhysRevLett.78.3410](https://doi.org/10.1103/PhysRevLett.78.3410).
- [Liu14a] Y.-k. Liu. Building one-time memories from isolated qubits. In *5th Conference on Innovations in Theoretical Computer Science - ITCS 2014*, pages 269–286, New York, New York, USA, 2014. ACM.
DOI: [10.1145/2554797.2554823](https://doi.org/10.1145/2554797.2554823).

- [Liu14b] Y.-K. Liu. Single-Shot Security for One-Time Memories in the Isolated Qubits Model. In *Advances in Cryptology – CRYPTO 2014*, volume 8617 PART 2 of *LNCS*, pages 19–36. Springer, 2014.
DOI: [10.1007/978-3-662-44381-1_2](https://doi.org/10.1007/978-3-662-44381-1_2).
- [Liu15] Y.-K. Liu. Privacy Amplification in the Isolated Qubits Model. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, volume 9057 of *LNCS*, pages 785–814. Springer, 2015.
DOI: [10.1007/978-3-662-46803-6_26](https://doi.org/10.1007/978-3-662-46803-6_26).
- [Lo97] H.-K. Lo. Insecurity of quantum secure computations. *Physical Review A*, 56: 1154–1162, 1997.
DOI: [10.1103/PhysRevA.56.1154](https://doi.org/10.1103/PhysRevA.56.1154).
- [May96] D. Mayers. The Trouble with Quantum Bit Commitment. *arXiv preprint quant-ph/9603015*, page 12, 1996.
arXiv: [quant-ph/9603015](https://arxiv.org/abs/quant-ph/9603015).
- [NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [Rab81] M. O. Rabin. How To Exchange Secrets with Oblivious Transfer. *Tech. Rep. TR-81, Aiken Comput. Lab, Harvard Univ.*, pages 1–5, 1981.
Online: <http://dm.ing.unibs.it/giuzzi/corsi/Support/papers-cryptography/187.pdf>.
- [RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2): 120–126, 1978.
DOI: [10.1145/359340.359342](https://doi.org/10.1145/359340.359342).
- [Sch10] C. Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Physical Review A*, 82(3): 032308, 2010.
DOI: [10.1103/PhysRevA.82.032308](https://doi.org/10.1103/PhysRevA.82.032308).
- [Sha49] C. E. Shannon. *Communication Theory of Secrecy Systems*. 1949.
- [Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science - FOCS 1994*, pages 124–134. IEEE, 1994.
DOI: [10.1109/SFCS.1994.365700](https://doi.org/10.1109/SFCS.1994.365700).
- [Wie83] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1): 78–88, 1983.
DOI: [10.1145/1008908.1008920](https://doi.org/10.1145/1008908.1008920). Originally written c. 1970 but unpublished.
- [Win99] A. Winter. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inf. Theory*, 45(7): 2481–2485, 1999.
DOI: [10.1109/18.796385](https://doi.org/10.1109/18.796385).
- [WST08] S. Wehner, C. Schaffner, and B. M. Terhal. Cryptography from Noisy Storage. *Physical Review Letters*, 100(22): 220502, 2008.
DOI: [10.1103/PhysRevLett.100.220502](https://doi.org/10.1103/PhysRevLett.100.220502).
- [Yao82] A. C. Yao. Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science - FOCS 1982*, pages 160–164. IEEE, 1982.
DOI: [10.1109/SFCS.1982.38](https://doi.org/10.1109/SFCS.1982.38).